XXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos
24 a 28 de maio de 2010
Gramado, RS

XV Workshop de Gerência e Operação de Redes e Serviços (WGRS)

Editora
Sociedade Brasileira de Computação (SBC)

Organizadores
Aldri Luiz dos Santos (UFPR)
Antônio Jorge Gomes Abelém (UFPA)
Luciano Paschoal Gaspary (UFRGS)
Marinho Pilla Barcellos (UFRGS)

Realização
Instituto de Informática
Universidade Federal do Rio Grande do Sul (UFRGS)

Promoção
Sociedade Brasileira de Computação (SBC)
Laboratório Nacional de Redes de Computadores (LARC)

Capa: Josué Klafke Sperb
Produção Editorial: Flávio Roberto Santos, Roben Castagna Lunardi, Matheus Lehmann, Rafael Santos Bezerra, Luciano Paschoal Gaspary e Marinho Pilla Barcellos.

Cópias Adicionais:
Sociedade Brasileira de Computação (SBC)
Av. Bento Gonçalves, 9500 - Setor 4 - Prédio 43.412 - Sala 219
Bairro Agronomia - CEP 91.509-900 - Porto Alegre - RS
Fone: (51) 3308-6835
E-mail: sbc@sbc.org.br

Dados Internacionais de Catalogação na Publicação (CIP)

Workshop de Gerência e Operação de Redes e Serviços (15. : 2010 : Gramado, RS).

Anais / XV Workshop de Gerência e Operação de Redes e Serviços; organizadores Aldri Luiz dos Santos... et al. − Porto Alegre : SBC, c2010.
199 p.

ISSN 2177-496X

1. Redes de computadores. 2. Sistemas distribuídos. I. dos Santos, Aldri Luiz. II. Título.

Promoção

Sociedade Brasileira de Computação (SBC)

Diretoria

Presidente
José Carlos Maldonado (USP)

Vice-Presidente
Marcelo Walter (UFRGS)

Diretor Administrativo
Luciano Paschoal Gaspary (UFRGS)

Diretor de Finanças
Paulo Cesar Masiero (USP)

Diretor de Eventos e Comissões Especiais
Lisandro Zambenedetti Granville (UFRGS)

Diretora de Educação
Mirella Moura Moro (UFMG)

Diretora de Publicações
Karin Breitman (PUC-Rio)

Diretora de Planejamento e Programas Especiais
Ana Carolina Salgado (UFPE)

Diretora de Secretarias Regionais
Thais Vasconcelos Batista (UFRN)

Diretor de Divulgação e Marketing
Altigran Soares da Silva (UFAM)

Diretor de Regulamentação da Profissão
Ricardo de Oliveira Anido (UNICAMP)

Diretor de Eventos Especiais
Carlos Eduardo Ferreira (USP)

Diretor de Cooperação com Sociedades Científicas
Marcelo Walter (UFRGS)

Promoção

Conselho

Mandato 2009-2013
Virgílio Almeida (UFMG)
Flávio Rech Wagner (UFRGS)
Silvio Romero de Lemos Meira (UFPE)
Itana Maria de Souza Gimenes (UEM)
Jacques Wainer (UNICAMP)

Mandato 2007-2011
Cláudia Maria Bauzer Medeiros (UNICAMP)
Roberto da Silva Bigonha (UFMG)
Cláudio Leonardo Lucchesi (UNICAMP)
Daltro José Nunes (UFRGS)
André Ponce de Leon F. de Carvalho (USP)

Suplentes - Mandato 2009-2011
Geraldo B. Xexeo (UFRJ)
Taisy Silva Weber (UFRGS)
Marta Lima de Queiroz Mattoso (UFRJ)
Raul Sidnei Wazlawick (UFSC)
Renata Vieira (PUCRS)

Laboratório Nacional de Redes de Computadores (LARC)

Diretoria

Diretor do Conselho Técnico-Científico
Artur Ziviani (LNCC)

Diretor Executivo
Célio Vinicius Neves de Albuquerque (UFF)

Vice-Diretora do Conselho Técnico-Científico
Flávia Coimbra Delicato (UFRN)

Vice-Diretor Executivo
Luciano Paschoal Gaspary (UFRGS)

Membros Institucionais
CEFET-CE, CEFET-PR, IME, INPE/MCT, LNCC, PUCPR, PUC-RIO, SESU/MEC, UECE, UERJ, UFAM, UFBA, UFC, UFCG, UFES, UFF, UFMG, UFPA, UFPB, UFPE, UFPR, UFRGS, UFRJ, UFRN, UFSC, UFSCAR, UNICAMP, UNIFACS, USP.

Realização

Comitê de Organização

Coordenação Geral
Luciano Paschoal Gaspary (UFRGS)
Marinho Pilla Barcellos (UFRGS)

Coordenação do Comitê de Programa
Luci Pirmez (UFRJ)
Thaís Vasconcelos Batista (UFRN)

Coordenação de Palestras e Tutoriais
Lisandro Zambenedetti Granville (UFRGS)

Coordenação de Painéis e Debates
José Marcos Silva Nogueira (UFMG)

Coordenação de Minicursos
Carlos Alberto Kamienski (UFABC)

Coordenação de Workshops
Antônio Jorge Gomes Abelém (UFPA)

Coordenação do Salão de Ferramentas
Nazareno Andrade (UFCG)

Comitê Consultivo
Artur Ziviani (LNCC)
Carlos André Guimarães Ferraz (UFPE)
Célio Vinicius Neves de Albuquerque (UFF)
Francisco Vilar Brasileiro (UFCG)
Lisandro Zambenedetti Granville (UFRGS)
Luís Henrique Maciel Kosmalski Costa (UFRJ)
Marcelo Gonçalves Rubinstein (UERJ)
Nelson Luis Saldanha da Fonseca (UNICAMP)
Paulo André da Silva Gonçalves (UFPE)

Realização

Organização Local
Adler Hoff Schmidt (UFRGS)
Alan Mezzomo (UFRGS)
Alessandro Huber dos Santos (UFRGS)
Bruno Lopes Dalmazo (UFRGS)
Carlos Alberto da Silveira Junior (UFRGS)
Carlos Raniery Paula dos Santos (UFRGS)
Cristiano Bonato Both (UFRGS)
Flávio Roberto Santos (UFRGS)
Jair Santanna (UFRGS)
Jéferson Campos Nobre (UFRGS)
Juliano Wickboldt (UFRGS)
Leonardo Richter Bays (UFRGS)
Lourdes Tassinari (UFRGS)
Luís Armando Bianchin (UFRGS)
Luis Otávio Luz Soares (UFRGS)
Marcos Ennes Barreto (UFRGS)
Matheus Brenner Lehmann (UFRGS)
Pedro Arthur Pinheiro Rosa Duarte (UFRGS)
Pietro Biasuz (UFRGS)
Rafael Pereira Esteves (UFRGS)
Rafael Kunst (UFRGS)
Rafael Santos Bezerra (UFRGS)
Ricardo Luis dos Santos (UFRGS)
Roben Castagna Lunardi (UFRGS)
Rodolfo Stoffel Antunes (UFRGS)
Rodrigo Mansilha (UFRGS)
Weverton Luis da Costa Cordeiro (UFRGS)

Mensagem dos Coordenadores Gerais

Bem-vindo(a) ao XXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2010)! Esta edição do simpósio está sendo realizada de 24 a 28 de maio de 2010 na pitoresca cidade de Gramado, RS. Promovido pela Sociedade Brasileira de Computação (SBC) e pelo Laboratório Nacional de Redes de Computadores (LARC) desde 1983, o SBRC 2010 almeja não menos que honrar com uma tradição de quase 30 anos: ser reconhecido como o mais importante evento científico em redes de computadores e sistemas distribuídos do país, e um dos mais concorridos em Informática. Mais do que isso, pretende estimular intercâmbio de idéias e discussões qualificadas, aproximá-lo(a) de temas de pesquisa efervescentes e fomentar saudável aproximação entre estudantes, pesquisadores, professores e profissionais.

Para atingir os objetivos supracitados, reunimos um grupo muito especial de professores atuantes em nossa comunidade que, com o nosso apoio, executou com êxito a tarefa de construir um **Programa Técnico** de altíssima qualidade. O SBRC 2010 abrange as seguintes atividades: 20 sessões técnicas de artigos completos, cobrindo uma grande gama de problemas em redes de computadores e sistemas distribuídos; 2 sessões técnicas para apresentações de ferramentas; 5 minicursos ministrados de forma didática, por professores da área, sobre temas atuais; 3 palestras e 3 tutoriais sobre tópicos de pesquisa avançados, apresentados por especialistas nacionais e estrangeiros; e 3 painéis versando sobre assuntos de relevância no momento. Completa a programação técnica a realização de 8 *workshops* satélites em temas específicos: WRNP, WGRS, WTR, WSE, WTF, WCGA, WP2P e WPEIF. Não podemos deixar de ressaltar o **Programa Social**, organizado em torno da temática "*vinho*", simbolizando uma comunidade de pesquisa madura e que, com o passar dos anos, se aprimora e refina cada vez mais.

Além da ênfase na qualidade do programa técnico e social, o SBRC 2010 ambiciona deixar, como marca registrada, seu esforço na busca por excelência organizacional. Tal tem sido perseguido há mais de dois anos e exigido muita determinação, dedicação e esforço de uma equipe afinada de organização local, composta por estudantes, técnicos administrativos e professores. O efeito desse esforço pode ser percebido em elementos simples, mas diferenciais, tais como uniformização de datas de submissão de trabalhos, portal *sempre* atualizado com as últimas informações, comunicação sistemática com potenciais participantes e pronto atendimento a qualquer dúvida. O nosso principal objetivo com essa iniciativa foi e continua sendo oferecer uma elevada *qualidade de experiência* a você, colega participante!

Gostaríamos de agradecer aos membros do Comitê de Organização Geral e Local que, por conta de seu trabalho voluntário e incansável, ajudaram a construir um evento que julgamos de ótimo nível. Gostaríamos de agradecer, também, à SBC, pelo apoio prestado ao longo das muitas etapas da organização, e aos patrocinadores, pelo incentivo à divulgação de atividades de pesquisa conduzidas no País e pela confiança depositada neste fórum. Por fim, nossos agradecimentos ao Instituto de Informática da UFRGS, por viabilizar a realização, pela quarta vez, de um evento do porte do SBRC.

Sejam bem-vindos à Serra Gaúcha para o "SBRC do Vinho"! Desejamos que desfrutem de uma semana agradável e proveitosa!

Luciano Paschoal Gaspary
Marinho Pilla Barcellos
Coordenadores Gerais do SBRC 2010

Mensagem do Coordenador do WGRS

O Workshop de Gerência e Operação de Redes e Serviços (WGRS) é um evento promovido anualmente pela Sociedade Brasileira de Computação (SBC) que se encontra na 15ª edição. O Workshop tem como objetivo atuar como um espaço para a apresentação de pesquisas e atividades relevantes na área de gerenciamento e operação de redes e serviços, integrando a comunidade brasileira de pesquisadores e profissionais atuantes nessa área. O Workshop visa, ainda, constituir um fórum para a apresentação e discussão de soluções utilizadas por provedores e usuários de sistemas de gerenciamento de redes.

Nesta edição, novos temas de interesse de comunidade foram incluídos na chamada de trabalhos, e a comunidade continuou a prestigiar o evento com um excelente número de submissões. De um total de 47 artigos submetidos, foram aceitos 14 para apresentação e publicação, representando uma taxa de aceitação inferior a 30%. O processo de avaliação dos artigos contou com a participação direta dos 26 membros do Comitê de Programa, alguns deles novos no comitê do programa, e de revisores associados a eles. Cada artigo foi avaliado por três especialistas na área.

Nos anais encontram-se os textos completos dos artigos selecionados, organizados em quatro sessões técnicas: (i) Monitoração e métodos baseados em metrologia de redes e Gerenciamento de redes ópticas, (ii) Aprovisionamento de redes e planejamento de capacidade, (iii) Gerenciamento de serviços e aplicações e (iv) Gerenciamento de redes móveis, sem fio e de sensores.

Eu gostaria de agradecer a todos os que ajudaram na preparação desse workshop, em particular aos membros do Comitê de Programa e demais revisores técnicos. Gostaria também de agradecer de forma especial o apoio da Coordenação do SBRC 2010, em particular aos coordenadores Luciano Paschoal Gaspary e Marinho Pilla Barcellos da Universidade Federal do Rio Grande do Sul (UFGRS) e ao coordenador dos workshops Antônio Jorge Gomes Abelém da Universidade Federal do Pará (UFPA). Por fim, gostaria de agradecer a coordenadora do WGRS 2009, Anelise Munaretto da Universidade Tecnológica Federal do Paraná (UTFPR), por sua colaboração compartilhando toda sua experiência na coordenação do WGRS.

Em nome do Comitê de Programa agradeço a todos os participantes do WGRS 2010, com os votos de um workshop bastante produtivo e agradável.

Aldri Luiz dos Santos
Coordenador do WGRS 2010

Comitê de Programa do WGRS

Aldri Luiz dos Santos, Universidade Federal do Paraná (UFPR)
Anelise Munaretto, Universidade Tecnológica Federal do Paraná (UTFPR)
Antônio Tadeu Azevedo Gomes, Laboratório Nacional de Computação Científica (LNCC)
Artur Ziviani, Laboratório Nacional de Computação Científica (LNCC)
Bruno Schulze, Laboratório Nacional de Computação Científica (LNCC)
Carlos Westphall, Universidade Federal de Santa Catarina (UFSC)
Célio Vinicius Neves de Albuquerque, Universidade Federal Fluminense (UFF)
Edmundo Madeira, Universidade Estadual de Campinas (UNICAMP)
Fátima Duarte-Figueiredo, Pontifícia Universidade Católica de Minas Gerais (PUC Minas)
Horacio Oliveira, Universidade Federal do Amazonas (UFAM)
Joaquim Celestino Júnior, Universidade Estadual do Ceará (UECE)
Jussara Almeida, Universidade Federal de Minas Gerais (UFMG)
Kelvin Dias, Universidade Federal do Pará (UFPA)
Linnyer Ruiz, Universidade Estadual de Maringá (UEM)
Lisandro Zambenedetti Granville, Universidade Federal do Rio Grande do Sul (UFRGS)
Luis Henrique Costa, Universidade Federal do Rio de Janeiro (UFRJ)
Luiz Nacamura Júnior, Universidade Tecnológica Federal do Paraná (UTFPR)
Luiz Henrique Correia, Universidade Federal de Lavras (UFLA)
Manoel Camillo de Oliveira Penna Neto, Pontifícia Universidade Católica do Paraná (PUCPR)
Marcelo Rubinstein, Universidade Estadual do Rio de Janeiro (UERJ)
Marcial Fernandez, Universidade Estadual do Ceará (UECE)
Mauro Fonseca, Pontifícia Universidade Católica do Paraná (PUCPR)
Michele Nogueira Lima, Universidade Federal do Paraná (UFPR)
Paulo André da Silva Gonçalves, Universidade Federal de Pernambuco (UFPE)
Raimir Holanda, Universidade de Fortaleza (UNIFOR)
Ronaldo Ferreira, Universidade Federal do Mato Grosso do Sul (UFMS)

Revisores do WGRS

Aldri Luiz dos Santos, Universidade Federal do Paraná (UFPR)
Anelise Munaretto, Universidade Tecnológica Federal do Paraná (UTFPR)
Antônio Tadeu Azevedo Gomes, Laboratório Nacional de Computação Científica (LNCC)
Artur Ziviani, Laboratório Nacional de Computação Científica (LNCC)
Bruno Schulze, Laboratório Nacional de Computação Científica (LNCC)
Carla Merkle Westphall, Universidade Federal de Santa Catarina (UFSC)
Carlos Senna, Universidade Estadual de Campinas (UNICAMP)
Carlos Raniery Paula dos Santos, Universidade Federal do Rio Grande do Sul (UFRGS)
Célio Vinicius Neves de Albuquerque, Universidade Federal Fluminense (UFF)
Clarissa Marquezan, Universidade Federal do Rio Grande do Sul (UFRGS)
Cristiano Both, Universidade Federal do Rio Grande do Sul (UFRGS)
Diego Passos, Universidade Federal Fluminense (UFF)
Efren Souza, Universidade Federal do Amazonas (UFAM)
Fátima Duarte-Figueiredo, Pontifícia Universidade Católica de Minas Gerais (PUC Minas)
Fernando Koch, University of Utrecht
Horacio Oliveira, Universidade Federal do Amazonas (UFAM)
Jéferson Nobre, Universidade Federal do Rio Grande do Sul (UFRGS)
Joaquim Celestino Júnior, Universidade Estadual do Ceará (UECE)
Jorge Lima de Oliveira Filho, Universidade Estadual de Campinas (UNICAMP)
Juliano Kazienko, Universidade Federal Fluminense (UFF)
Jussara Almeida, Universidade Federal de Minas Gerais (UFMG)
Kelvin Dias, Universidade Federal do Pará (UFPA)
Linnyer Ruiz, Universidade Estadual de Maringá (UEM)
Lisandro Zambenedeti Granville, Universidade Federal do Rio Grande do Sul (UFRGS)
Luciano Chaves, Universidade Estadual de Campinas (UNICAMP)
Luis Henrique Costa, Universidade Federal do Rio de Janeiro (UFRJ)
Luiz Nacamura Júnior, Universidade Tecnológica Federal do Paraná (UTFPR)
Luiz Henrique Correia, Universidade Federal de Lavras (UFLA)
Manoel Camillo de Oliveira Penna Neto, Pontifícia Universidade Católica do Paraná (PUCPR)
Marcelo Rubinstein, Universidade Estadual do Rio de Janeiro (UERJ)
Marcelo Luiz Drumond Lanza, Universidade Federal do Rio de Janeiro (UFRJ)
Marcial Fernandez, Universidade Estadual do Ceará (UECE)
Marcos Assunção, University of Melbourne
Mauro Fonseca, Pontifícia Universidade Católica do Paraná (PUCPR)
Michele Nogueira Lima, Universidade Federal do Paraná (UFPR)
Miguel Elias Mitre Campista, Universidade Federal do Rio de Janeiro (UFRJ)
Neumar Malheiros, Universidade Estadual de Campinas (UNICAMP)
Paulo André da Silva Gonçalves, Universidade Federal de Pernambuco (UFPE)
Rafael dos Santos Alves, Universidade Federal do Rio de Janeiro (UFRJ)
Rafael Esteves, Universidade Federal do Rio Grande do Sul (UFRGS)
Raimir Holanda, Universidade de Fortaleza (UNIFOR)
Ricardo Carrano, Universidade Federal Fluminense (UFF)
Ronaldo Ferreira, Universidade Federal do Mato Grosso do Sul (UFMS)
Thais Braga, Universidade Federal de Minas Gerais (UFMG)

Sumário

Sessão Técnica 1 – Monitoração e Métodos Baseados em Metrologia de Redes e Gerenciamento de Redes Ópticas

Caracterização de Padrões de Uso do Protocolo SNMP
Ewerton Monteiro Salvador, Jussara M. Almeida, José Marcos Silva Nogueira (UFMG), Lisandro Zambenedetti Granville e Paulo Eduardo Barbosa (UFRGS) 3

Análise de Uso e Mobilidade em uma Rede sem Fio Urbana de Larga Escala
Fernanda Vilas Boas Fuscaldi e Cristina Duarte Murta (CEFET-MG) 17

Monitoração de qualidade de serviço de redes com aplicações de tempo-real utilizando técnicas de amostragem baseadas em CEP
Renata M. S. Wowk e Edgard Jamhour (PUCPR)..... 29

Desempenho do Roteamento Adaptativo-Alternativo em Redes Ópticas Dinâmicas
Paulo Ribeiro L. Júnior (UFCG), Michael Taynnan (IFPB) e Marcelo S. Alencar (UFCG) 43

Sessão Técnica 2 – Aprovisionamento de Redes e Planejamento de Capacidade

Planejamento de Redes em Malha Sem Fio Lineares
Felipe Rolim e Souza e Célio V. N. Albuquerque (UFF)..... 59

Proposta de Método para Engenharia de Tráfego em Redes *Mesh*
Andrey Juliano Fischer e Edgard Jamhour (PUCPR) 73

Projeto de Topologia Virtual em Redes Ópticas: Uma Abordagem para Evitar a Interferência entre Canais
K. D. R. Assis (UFBA), M. S. Savasini (UNICAMP), A. F. Santos (USP) e W. F. Giozza (UnB) 87

Sessão Técnica 3 – Gerenciamento de Serviços e Aplicações

Similaridade para Avaliação de Riscos em Planos de Mudança de TI
Luis Armando Bianchin, Juliano Araujo Wickboldt, Ricardo Luis dos Santos, Roben Castagna Lunardi, Bruno Lopes Dalmazo, Fabricio Girardi Andreis, Weverton Luis da Costa Cordeiro, Abraham Lincoln Rabelo de Sousa, Lisandro Zambenedetti Granville e Luciano Paschoal Gaspary (UFRGS)..... 103

Using a Cloud-based Event Service for Managing Context Information in Mobile and Ubiquitous Systems
Waldir R. Pires Junior, Antonio A. F. Loureiro (UFMG) e Ricardo A. R. Oliveira (UFOP) 117

Filtro de Conteúdo para Sistemas SMS Baseado em Classificador Bayesiano e Agrupamento por Palavras
Dirceu Belém e Fátima Duarte-Figueiredo (PUC Minas)..... 131

Sessão Técnica 4 – Gerenciamento de Redes Móveis, Sem Fio e de Sensores

Proposta De Uma Métrica de Roteamento Para Redes *Wireless Mesh* com Tráfego *Voip*
Cleverton Juliano Alves Vicentini, Roberson Cesar Alves de Araujo e Mauro Sergio Pereira Fonseca (PUCPR)..... 147

Abaré: Um Framework para Implantação, Monitoramento e Gerenciamento Coordenado e Autônomo para Redes em Malha sem Fio
Billy Anderson Pinheiro, Vagner de Brito Nascimento, Eduardo Cerqueira, Antônio Jorge Gomes Abelém (UFPA) e Augusto Neto (UFG) 157

LiTE: Um Algoritmo de Localização Temporal e Ordenação de Eventos em Redes de Sensores Sem Fio Compostas por Nós Dessincronizados
Leonardo L. Guimarães, Horácio A. B. F. Oliveira (UFAM), Rômulo T. Rodrigues (Universidade do Porto), Edjair S. Mota (UFAM) e Antonio A. F. Loureiro (UFMG)..... 171

Maximização da vida útil de redes de sensores sem fio utilizando fusão de dados e roteamento *fuzzy*
Rafael Lopes Gomes, Thiego Nunes, Dionne Monteiro e Antônio Gomes Abelém (UFPA) 185

Índice por Autor 199

XV Workshop de Gerência e Operação de Redes e Serviços

♦

Sessão Técnica 1

Monitoração e Métodos Baseados em Metrologia de Redes e Gerenciamento de Redes Ópticas

Caracterização de Padrões de Uso do Protocolo SNMP*

Ewerton Monteiro Salvador[1], Jussara M. Almeida[1], José Marcos Silva Nogueira[1], Lisandro Zambenedetti Granville[2], Paulo Eduardo Barbosa[2]

[1] Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)
Av. Antônio Carlos, 6627 – ICEx – Belo Horizonte, MG

{ewerton, jussara, jmarcos}@dcc.ufmg.br

[2]Instituto de Informática
Universidade Federal do Rio Grande do Sul (UFRGS)
Av. Bento Gonçalves, 9500 – Porto Alegre, RS

{granville, pauloctb}@inf.ufrgs.br

Abstract. *The Simple Network Management Protocol (SNMP), proposed almost 20 years ago, still remains as the de facto standard for managing of TCP/IP networks. However, there are few studies that present the real use of SNMP in production networks. This work aims at contributing with the efforts carried out by the network management community in order to improve the knowledge about the use of SNMP by presenting the characterization results of a sample of the management traffic from the Brazilian RNP network. The presented results may guide the development of new technologies for managing networks, in order to better meet the needs of the production networks users.*

Resumo. *O Simple Network Management Protocol (SNMP), proposto há quase 20 anos, continua sendo o padrão de facto para gerenciamento de redes TCP/IP. Contudo, ainda são poucos os estudos que descrevem a real utilização do SNMP em redes em produção. Visando contribuir com os esforços da comunidade de gerenciamento de redes para melhorar a compreensão da utilização do protocolo, este trabalho apresenta os resultados da caracterização de uma amostra do tráfego de gerenciamento da RNP, no Brasil. Os resultados apresentados podem direcionar o desenvolvimento de novas tecnologias para o gerenciamento de redes, a fim de melhor atender as necessidades dos usuários das redes em produção.*

1. Introdução

Na última década, um conjunto de novos estudos estão sendo conduzidos na área de gerenciamento de redes a fim de investigar o quão adequadas são as técnicas de gerenciamento existentes frente às características atuais das redes de computadores. Dentre os resultados que vêm sendo alcançados a partir desses estudos, destacam-se aqueles que buscam descentralizar a tarefa de gerenciamento de redes, seja utilizando tecnologias alternativas, como Web Services [Curbera et al. 2002] ou redes P2P

*Os autores deste artigo agradecem o apoio fundamental do CNPq, da FAPEMIG e da CAPES para a realização deste trabalho, assim como a disponibilidade da RNP para o fornecimento da amostra de tráfego SNMP aqui estudada.

[Androutsellis-Theotokis and Spinellis 2004], ou criando novos modelos, como o modelo de gerenciamento por delegação [Goldszmidt and Yemini 1995] ou o modelo de gerenciamento baseado em políticas [Westerinen et al. 2001]. Contudo, o padrão *de facto* para gerenciamento de redes TCP/IP continua sendo o *Simple Network Management Protocol* (SNMP) [Case et al. 1990], o qual foi proposto há quase 20 anos e permanece sendo amplamente utilizado.

Diversas publicações recentes têm por objetivo principal a identificação de padrões de utilização do SNMP por meio de medições de tráfegos de gerenciamento de redes em produção. A principal motivação por trás desses estudos é o fato de que ainda hoje pouco se conhece sobre a forma como o SNMP é efetivamente utilizado em redes reais. Este fato é prejudicial para a comunidade de gerenciamento de redes como um todo, pois a falta desse conhecimento leva os pesquisadores e desenvolvedores a fazerem pressuposições sobre o comportamento do protocolo, o que enfraquece a base sobre a qual novas tecnologias estão sendo propostas e desenvolvidas. Atualmente, já existe uma metodologia bem definida para a realização desse tipo de estudo [Schoenwaelder 2008], e alguns interessantes resultados preliminares já foram publicados em veículos relevantes [Schönwälder et al. 2007] [Salvador and Granville 2008a] [Salvador and Granville 2008b]. Exemplos de questões que estão sendo investigadas são: quais recursos do SNMP (ex.: versões, operações, MIBs - *Management Information Bases*) estão sendo utilizados; como o uso do SNMP difere nos vários tipos existentes de redes das organizações; quais informações são mais frequentemente requisitadas e quais são as interações mais típicas que estão sendo empregadas? Contudo, os resultados conhecidos até o presente momento não são exaustivos, e uma série de características acerca da utilização do SNMP demandam investigações mais profundas a fim de se alcançar resultados mais concretos, tais como: identificação de componentes periódicos e aperiódicos nos tráfegos, correlações existentes entre tipos de mensagens distintos com possíveis relações causa-efeito, potencial para otimização do consumo de banda e do balanceamento de carga do tráfego de gerenciamento, aplicações reais para o uso de *traps*, entre outras.

Neste contexto, este trabalho objetiva contribuir com novos resultados acerca da utilização do SNMP nas redes em produção. Para tanto, foi estudado um tráfego de gerenciamento SNMP da Rede Nacional de Ensino e Pesquisa (RNP). Uma série de técnicas de análises quantitativas foram empregadas sobre uma amostra do tráfego, a fim de se caracterizar a utilização do SNMP quanto a aspectos tais como periodicidade de diversos componentes do tráfego, correlações entre tipos de mensagens encontradas nos diversos dias de tráfego monitorado, relação entre o uso de traps e os eventos ocorridos na rede dentro da amostra de tráfego coletada e níveis de centralização do tráfego de gerenciamento da RNP.

O restante deste artigo está organizado da seguinte maneira. A Seção 2 apresenta os trabalhos que estão relacionados a este artigo. Já a Seção 3 destaca o conjunto de técnicas que compuseram a metodologia empregada para as medições sobre o tráfego da RNP estudado, enquanto que a Seção 4 detalha os resultados que foram obtidos a partir do estudo realizado. Por fim, a Seção 5 apresenta conclusões e trabalhos futuros.

2. Trabalhos relacionados

Devido ao fato da metodologia proposta pelo IRTF (*Internet Research Task Force*) para medições de tráfegos SNMP ser relativamente nova, atualmente existem poucos trabalhos contendo resultados acerca dos padrões de utilização do protocolo de gerenciamento nas redes em produção. O primeiro artigo relacionado a este tema foi publicado em 2007, pelo próprio autor da metodologia do IRTF, em parceria com outros pesquisadores [Schönwälder et al. 2007] e consistiu numa coletânea de resultados preliminares de medições realizadas sobre oito tráfegos SNMP coletados. Dentre as principais conclusões do trabalho, encontram-se os fatos de que o SNMP é utilizado primeiramente para monitoramento e não para configuração e que, apesar de o SNMPv3 ser o padrão atual para gerenciamento de redes TCP/IP, o mesmo foi pouco visto nos tráfegos estudados.

Já em 2008, foi publicado o trabalho de Salvador e Granville [Salvador and Granville 2008a], no qual foram realizadas algumas medições sobre uma amostra do tráfego de gerenciamento do Ponto-de-Presença (POP) da Rede Nacional de Ensino e Pesquisa (RNP) no Rio Grande do Sul. No mesmo ano, um novo trabalho [Salvador and Granville 2008b] foi publicado por esses mesmos autores, onde a amostra de tráfego estudada foi a da Rede Nacional de Pesquisa (RNP) como um todo, ao invés de apenas um POP (caso da publicação anterior). Uma característica comum desses dois trabalhos é que os mesmos tinham como foco principal um conjunto de propostas de técnicas de visualização para serem utilizadas em conjunto com a metodologia proposta pelo IRTF, a fim de facilitar o processo de interpretação dos resultados obtidos a partir das medições realizadas sobre um tráfego SNMP. Nesse contexto, as análises realizadas sobre os tráfegos do POP da RNP no Rio Grande do Sul e da própria rede da RNP como um todo tiveram por objetivo principal validar as técnicas de visualização proposta. Devido a isso, os tráfegos estudados nos trabalhos anteriores ainda não foram extensivamente analisados, fato este que consiste numa interessante oportunidade de pesquisa que está sendo explorada no presente artigo.

Em 2009 os pesquisadores Dobrev e Stancu-Mara [Dobrev et al. 2009], em colaboração com o autor da metodologia do IRTF, Schoenwaelder, passaram a investigar técnicas de visualização que melhor representassem a interação entre nós presentes num determinado tráfego de gerenciamento SNMP. Nesse trabalho, foram avaliadas a utilização de duas ferramentas de visualização (*network animator* - nam, e NetViz/JUNG) em conjunto com tráfegos SNMP representados nos formatos definidos pela metodologia do IRTF para medições de tráfegos SNMP. Esse trabalho se relaciona com o presente artigo no que diz respeito à constante busca pela identificação de padrões de utilização através de análises sobre tráfegos de gerenciamento de redes.

3. Metodologia utilizada nas medições sobre o tráfego SNMP

Para a realização das medições sobre o tráfego SNMP da Rede Nacional de Ensino e Pesquisa (RNP), foram utilizadas a metodologia do IRTF para medições de tráfegos SNMP [Schoenwaelder 2008] e um conjunto de técnicas de análise quantitativa. Os quatro primeiros passos citados na metodologia do IRTF já foram previamente realizados, sendo eles: captura do tráfego de gerenciamento, conversão dos arquivos PCAP para o formato CSV (*Comma Separated Values*), filtragem dos arquivos CSV para remoção de dados sensíveis (ex.: *strings* de comunidade e endereços IP de gerentes e agentes) e armazenamento dos arquivos PCAP e CSV em um repositório estável para os casos em que um

retorno aos dados originais seja necessário. Os esforços dos quais este artigo é resultante foram concentrados no quinto passo da metodologia do IRTF, que consiste na realização de análises sobre o arquivo de tráfego no formato CSV, através da execução de programas e *scripts*, a fim de se caracterizar a utilização do protocolo SNMP nas redes em produção.

Objetivando-se compreender os padrões de utilização do SNMP na rede de gerenciamento da RNP, as seguintes métricas foram selecionadas: distribuição dos diversos tipos de mensagens de gerenciamento trocadas entre gerentes e agentes da rede, distribuição de acessos a objetos e MIBs utilizados e periodicidade do tráfego de gerenciamento. A escolha das mesmas se deu pela grande quantidade de informações acerca do uso do SNMP no tráfego estudado que pode ser obtida a partir desse conjunto de métricas. Como exemplo citam-se: pontos de concentração de tráfego de gerenciamento na rede, justificativas para o uso das diversas operações encontradas no tráfego identificadas a partir das informações acessadas nos agentes da rede, componentes periódicos e aperiódicos na distribuição das operações realizadas pelo SNMP na rede da RNP, entre outros.

Com relação às técnicas de análise quantitativa empregadas no estudo do SNMP na RNP, foi feita uma caracterização do tráfego estudado, apresentando as distribuições dos números dos diversos tipos de mensagens SNMP presentes no tráfego, tais como *get-request*, *response*, *get-next-request*, *trap*, entre outras. Foram ainda analisadas as correlações entre os números de mensagens de cada tipo e o número de mensagens de mesmo tipo em diferentes dias em que houve monitoramento de tráfego na rede da RNP.

Conforme já mencionado anteriormente, a carga de trabalho escolhida para a execução das análises foi o tráfego de gerenciamento SNMP da RNP. Esse tráfego é o produto de 14 dias de monitoramento no núcleo da rede da instituição, ocorrido entre os dias 22 de junho e 5 de julho de 2007. Uma vez que os autores deste trabalho já tinham a disposição essa amostra de tráfego, a mesma foi selecionada, também, devido à sua disponibilidade, além do fato da mesma ser representativa no cenário brasileiro de redes de computadores. As características gerais do tráfego SNMP são apresentadas na Tabela 1.

Tabela 1. Características gerais da amostra de tráfego estudada

Início da amostra:	2007-06-22T22:10:03+0000
Fim da amostra:	2007-07-06T22:10:56+0000
Duração do trace:	14 dias 0 horas 0 minutos
Quantidade de mensagens:	30.674.350
Quantidade de gerentes:	6
Quantidade de agentes	100

Uma particularidade a ser mencionada nesse tráfego é a pequena quantidade de mensagens capturadas no segundo dia do monitoramento (23 de junho de 2007). Isso ocorreu devido a um problema durante o processo de captura dos pacotes SNMP, ocasionando o corrompimento do arquivo PCAP (resultante da captura de pacotes pelo *sniffer* de rede). Contudo, esse estudo considera todas as mensagens SNMP capturadas neste dia e que não foram corrompidas por esta falha, a fim de se extrair o máximo da amostra obtida.

4. Resultados

Os resultados obtidos a partir da presente pesquisa serão detalhados nas próximas subseções da seguinte forma: primeiramente serão apresentados dados sobre o uso do SNMP na rede da RNP de um modo geral. Em seguida, serão caracterizadas as diversas operações do SNMP que foram observadas na amostra estudada. Por fim, serão discutidas as correlações percebidas entre as diversas operações do protocolo.

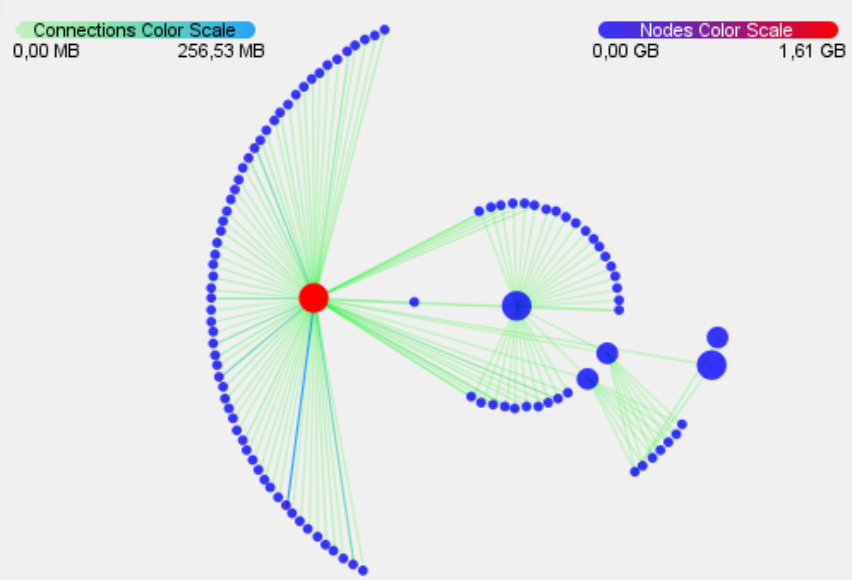


Figura 1. Topologia de gerenciamento SNMP da rede da RNP

Na Figura 1, onde é apresentada a topologia de gerenciamento percebida na RNP, pode-se notar que a maior parte do tráfego de gerenciamento está concentrado em torno de um único gerente, o qual encontra-se colorido de vermelho por concentrar a maior quantidade de tráfego. Todo o tráfego desse gerente principal consiste exclusivamente de mensagens de polling do protocolo SNMP (`get-request`, `get-next-request`, `get-bulk-request` e `response`). As mensagens do tipo `trap` estão todas concentradas no segundo maior gerente da rede, que está representado na figura como o círculo grande azul imediatamente à direita do gerente principal. Esse gerente também é exclusivamente utilizado para lidar com mensagens do tipo `trap`. Os demais fluxos de mensagens são menos representativos, muito provavelmente porque os mesmos tiveram uma participação esporádica no processo de gerenciamento da rede da RNP ao longo dos dias em que houve monitoramento. Assim, a caracterização do tráfego é focada principalmente no tráfego concentrado nesses 2 principais gerentes da rede e os agentes interconectados a esses nós.

4.1. Distribuição da quantidade de mensagens no tráfego

Um dos *scripts* de análise que acompanham a ferramenta SNMPDUMP [Schoenwaelder 2008], utilizada na conversão de formatos de tráfego na metodologia do IRTF, gera um relatório apresentando a distribuição do número dos vários tipos de mensagens e também as versões utilizadas do protocolo SNMP. Esse *script* foi executado sobre todo o tráfego da RNP monitorado, a fim de se obter uma visão geral da distribuição das mensagens de gerenciamento. O resultado obtido está representado na Tabela 2.

Tabela 2. Tipos e versões das mensagens no tráfego da RNP

Tipo de mensagem	Versão do SNMP	Quantidade
get-request	SNMPv1	940.491
get-request	SNMPv2c	11.574.343
get-next-request	SNMPv1	2.154.137
get-next-request	SNMPv2c	7.032
get-bulk-request	SNMPv2c	774.570
trap	SNMPv1	6.614
trap	SNMPv2c	107.977
response	SNMPv1	2.777.042
response	SNMPv2c	12.332.123

Nota-se que não foram observadas mensagens SNMPv3 no tráfego analisado. A explicação mais provável para isso é a ausência de implementação desta versão do SNMP na maioria dos dispositivos de rede disponíveis na rede da RNP. Outro fato interessante é o baixo uso de *traps* no tráfego estudado, em comparação com as outras operações observadas. Isso mostra uma subutilização de um recurso com potencial para reduzir substancialmente a sobrecarga causada pelo tráfego de gerenciamento, através da substituição da técnica de *polling*, com requisições e respostas constantes, pela técnica de notificação. Por fim, é fácil identificar que a versão predominante do SNMP no tráfego estudado é a SNMPv2c, que por sua vez está presente na maioria dos atuais dispositivos de redes com capacidade de gerenciamento disponíveis no mercado. Apesar da versão 2 do protocolo SNMP já disponibilizar formas de reduzir a quantidade de mensagens de *polling* na rede, com a introdução da operação `get-bulk-request`, existe o lado negativo de uma grande deficiência na segurança das operações realizadas através do protocolo, que só foram sanadas na versão 3 do mesmo.

4.2. MIBs e sub-árvores mais acessadas no tráfego

Através da execução de um *script* específico, observou-se também a distribuição de acessos a objetos de gerenciamento e MIBs SNMP ao longo de todo o tráfego monitorado. Na Tabela 3 estão listadas as 10 MIBs e suas respectivas sub-árvores de objetos mais acessadas no tráfego estudado. O objetivo desta análise também foi permitir uma melhor compreensão das características básicas do tráfego, a fim de se adequar melhor as técnicas empregadas.

A partir dos dados da Tabela 3 pode-se observar que a maior parte dos acessos são a objetos da `MIB-2`, que é uma MIB padronizada pelo IETF. Nesta MIB, a sub-árvore mais acessada é a `interfaces`, que fornece informações sobre o estado da interface de rede do dispositivo monitorado, o que indica que provavelmente está se realizando *polling* sobre esses dispositivos para se saber o estado de funcionamento dos mesmos. Nota-se também que algumas MIBs não padronizadas também estão sendo utilizadas, como a `enterprises/cisco` e a `enterprises/ucd-snmp`, o que demonstra que nem sempre administradores optam por utilizar MIBs padronizadas em detrimento das MIBs fornecidas pelos fabricantes dos dispositivos utilizados.

Tabela 3. MIBs mais acessadas no tráfego da RNP

MIB/Sub-árvore	Número de Acessos
mib-2/interfaces	28.478.953
mib-2/ifMIB	8.427.996
mib-2/system	2.943.137
mib-2/ip	2.740.604
enterprises/cisco	902.246
enterprises/ucd-snmp	856.915
enterprises/2636	721.492
mib-2/bgp	331.264
snmpModules/snmpMIB	168.933
mib-2/ospf	149.936

4.3. Caracterização das operações do SNMP na rede da RNP

A partir desta subseção serão detalhadas algumas características do uso das operações do SNMP na rede da RNP, a partir da análise das distribuições das mensagens ao longo da amostra de tráfego estudada. As distribuições foram organizadas de duas formas distintas: uma leva em consideração a quantidade de mensagens por operações amostradas a cada 15 minutos (ex.; o ponto 0 representa a quantidade de mensagens observadas entre 00h:00m:00s e 00h:14m:59s, enquanto que o ponto 15 representa a quantidade de mensagens entre 00h:15m:00s e 00h:29m:59s, e assim por diante), enquanto que a outra considera a quantidade de mensagens de cada operação amostrada a cada 1 minuto. A primeira visa oferecer uma visão de mais alto nível da utilização agregada das operações do SNMP, enquanto a segunda é utilizada sempre que se faz necessária a visualização de partes do tráfego num maior nível de detalhamento, a fim de se encontrar explicações para observações que não são evidentes a partir da distribuição amostrada a cada 15 minutos.

`Mensagens get-request`

A distribuição do número de mensagens da operação `get-request` no tráfego é relativamente constante ao longo de todos os dias presentes na amostra de tráfego. Nas medições realizadas no dia 26 de junho de 2007, ilustrada na Figura 2, a média da ocorrência de mensagens `get-request` em intervalos de 15 minutos é 10.337,67, o desvio padrão é 55,87, e o coeficiente de variação é apenas 0,0054. Uma vez que esses valores são representativos para todo o tráfego, conclui-se que, de um modo geral, a variação no tráfego de mensagens `get-request` é muito pequena. Contudo, observa-se um aumento na variação da quantidade de mensagens `get-request` a partir das 12:00h de todos os dias em que houve monitoramento do tráfego neste horário. Este comportamento está ilustrado na Figura 2, que mostra a variação do número de mensagens `get-request` em intervalos de 15 minutos em um dia específico da carga analisada. Note que o valor 0 não foi incluído no eixo y, uma vez que a ordem de grandeza desses valores para a operação `get-request` é muito superior à das demais operações observadas na rede da RNP. Além disso, o uso de uma escala muito grande esconderia a variação que ocorre a partir do ponto 720 (12:00h). Apesar dessa variação ser pequena, é clara a mudança de padrão da curva a partir das 12:00h.

A possível razão para a pequena variação que ocorre a partir das 12:00h é o aci-

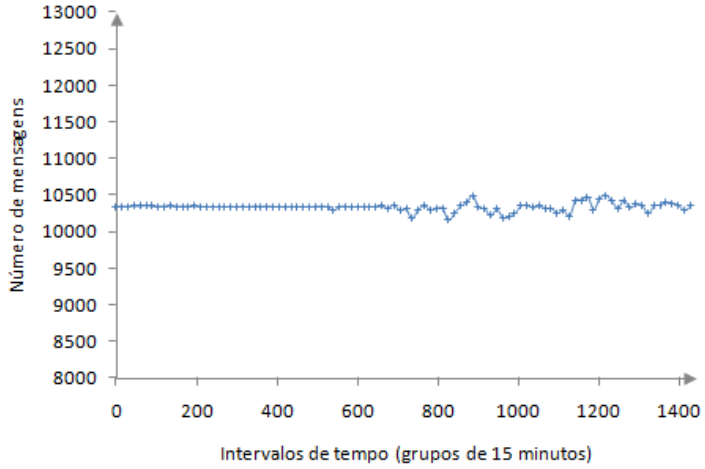


Figura 2. Distribuição do número de mensagens `get-request` amostrada em intervalos de 15 minutos, observada no dia 26 de junho de 2007

onamento de rotinas de *polling* por parte dos sistemas de gerenciamento a partir deste horário. Contudo, esperava-se uma maior periodicidade das solicitações, fato que não ocorre no tráfego estudado, uma vez que não é possível se estabelecer um padrão claro na distribuição da quantidade de mensagens a partir das 12h. Uma investigação mais profunda, em conjunto com os administradores da rede da RNP, se faz necessária, afim de se esclarecer a razão por trás desse comportamento.

Uma investigação mais detalhada foi realizada na parte mais constante do tráfego de mensagens `get-request`. A distribuição do número de mensagens amostradas em intervalos de 1 minuto no período das 03h até as 04:30h está representada na Figura 3. A partir da análise desta figura observa-se que, de fato, no período que antecede às 12h, o tráfego de mensagens `get-request` é bastante periódico, o que pode ser explicado pelo fato de que a RNP utiliza ferramentas de gerenciamento que realizam *polling* nos dispositivos e serviços gerenciados em intervalos de tempo pré-fixados, de forma periódica.

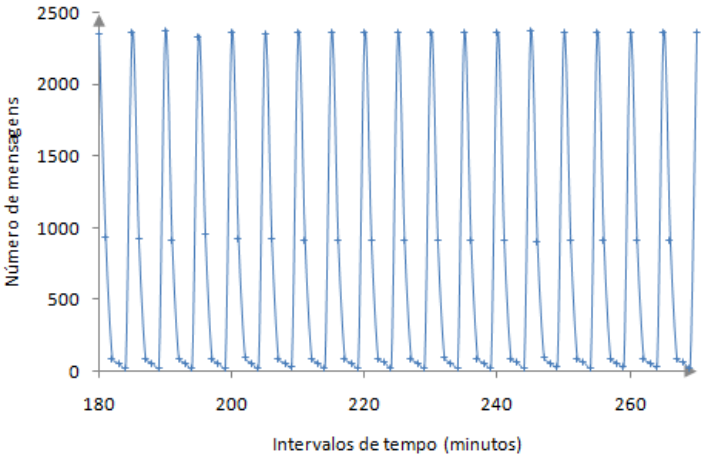


Figura 3. Distribuição do número de mensagens `get-request` amostrada em intervalos de 1 minuto, observada entre as 3h e 4:30h do dia 26 de junho de 2007

Mensagens get-next-request

Mensagens `get-next-request` são utilizadas para serem realizados caminhamentos em árvores MIB, e a utilização deste tipo de caminhamento é bastante comum em softwares de gerenciamento que realizam *polling* sobre os objetos gerenciados. Devido a essas características, é esperado que o tráfego de mensagens `get-next-request` seja mais periódico. Observou-se que a amostra de tráfego da rede da RNP também segue essa tendência em todos os dias em que houve monitoramento, conforme demonstrado na Figura 4.

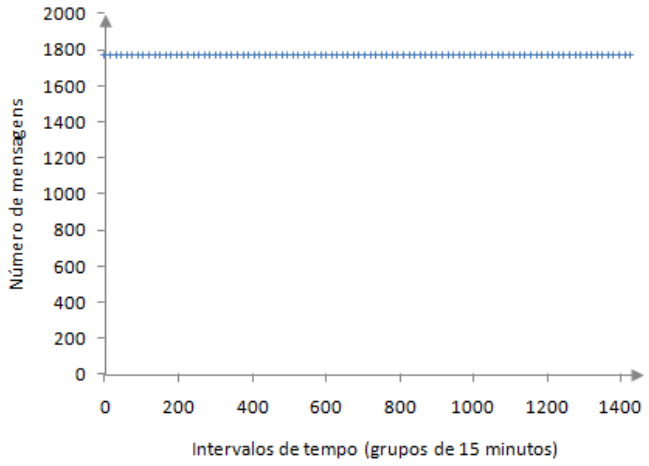


Figura 4. Distribuição do número de mensagens `get-next-request` amostrada em intervalos de 15 minutos, observada no dia 04 de julho de 2007

No dia retratado na Figura 4, observou-se que a média da distribuição da quantidade de mensagens em intervalos de 15 minutos foi de 1.770,16 mensagens, o desvio padrão foi de 0,79 e o coeficiente de variação de variação foi 0,0004. Com isso, ressalta-se ainda mais a periodicidade do tráfego de mensagens `get-next-request` observada na rede da RNP, uma vez que valores bastantes próximos desses que foram apresentados se repetem ao longo de todos os dias em que houve monitoramento de tráfego.

get-bulk-request

A operação `get-bulk-request` foi definida na versão 2 do SNMP, e tem função semelhante à da operação `get-next-request`. Basicamente, esse tipo de mensagem solicita a um agente a recuperação de valores de vários objetos simultaneamente. A diferença entre o `get-bulk-request` e o `get-next-request` é que no `get-bulk-request` é possível o transporte de valores de várias instâncias de um mesmo objeto, diminuindo assim a sobrecarga do SNMP sobre a rede. Por conta desse comportamento, esta operação também é muito utilizada na função de `polling` pelos sistemas de gerenciamento, o que resulta na expectativa da distribuição de mensagens desse tipo ter um comportamento periódico. Mais uma vez esse comportamento pôde ser observado ao longo de todo o tráfego da RNP estudado, conforme mostra a Figura 5.

No dia 29 de junho, retratado na Figura 5, registrou-se uma média de distribuição de mensagens em intervalos de 15 minutos de 589,82 mensagens, desvio padrão de 12,80 e coeficiente de variação de 0,02171. Mais uma vez, isso demonstra um comporta-

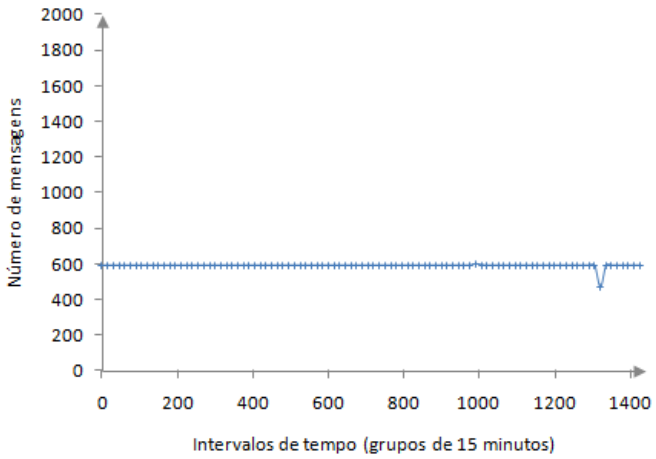


Figura 5. Distribuição do número de mensagens `get-bulk-request` amostrada em intervalos de 15 minutos, observada no dia 29 de junho de 2007

mento bastante constante nessa distribuição, a qual se repete em todos os dias do tráfego monitorado, porém em proporção bem menor em relação às operações `get-request` e `get-next-request`. A utilização de mensagens do tipo `get-bulk-request` é mais econômica do que os tipos `get-request` e `get-next-request` pelo fato de ser necessário, na maioria dos casos, apenas um único cabeçalho de mensagem para a recuperação de valores de vários objetos, ao contrário do que ocorre nos dois outros tipos de mensagem (um cabeçalho para um valor recuperado). Este fato mostra que existe um potencial de diminuição da sobrecarga do tráfego de gerenciamento na rede estudada.

Um ponto que chama atenção no gráfico da Figura 5 ocorre nas proximidades do ponto 1.320 (correspondente ao período entre as 22h:00m:00s e 22h:14m:59s), onde percebe-se um valor anormalmente baixo, em comparação com os outros valores do gráfico. Este declive é uma constante em todos os dias onde o tráfego de gerenciamento da RNP foi monitorado, sempre no mesmo horário, o que indica que muito provavelmente se trata de um comportamento pré-programado no sistema de gerenciamento da rede. Outras investigações se fazem necessárias para melhor explicar o fenômeno observado.

`trap`

Na amostra de tráfego estudada puderam ser observadas mensagens do tipo `trap` das versões 1 e 2 do protocolo SNMP. Uma vez que o mecanismo de traps é assíncrono, espera-se que a distribuição da quantidade dessas mensagens tenha um caráter mais aperiódico, uma vez que elas só são enviadas na rede mediante a ocorrência de algum evento específico. Essa expectativa foi concretizada no estudo realizado sobre o tráfego SNMP da rede da RNP. Um exemplo típico do comportamento das mensagens do tipo `trap` desse tráfego encontra-se representado na Figura 6.

Uma das coisas que se percebe ao se analisar a Figura 6 é a existência de picos que se destacam em relação a um patamar inferior de quantidade de mensagens do tipo `trap`. A existência desses picos indicam possíveis problemas que ocorreriam no instante em que os mesmos aparecem, uma vez que mensagens do tipo `trap` são enviadas na ocorrência de um evento relevante para o gerenciamento da rede. Dentre os principais problemas

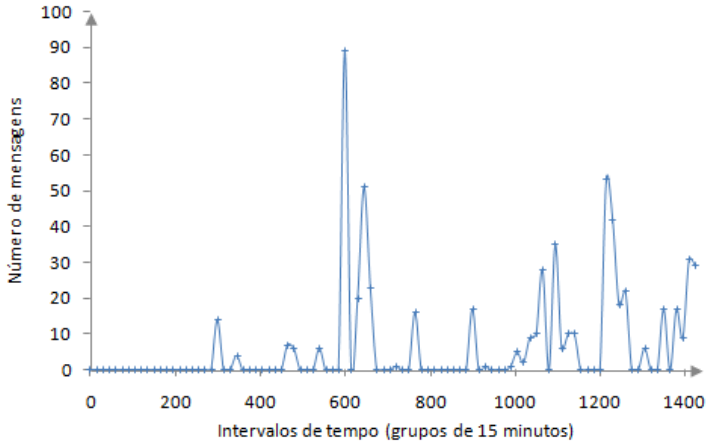


Figura 6. Distribuição do número de mensagens `trap` amostrada em intervalos de 15 minutos, observada no dia 26 de junho de 2007

reportados nas mensagens de `trap`, encontram-se falhas de autenticação e problemas com o protocolo de roteamento BGP.

A variação na distribuição de mensagens do tipo `trap` é sempre muito alta em todos os dias onde houve monitoramento do tráfego de gerenciamento da RNP. No caso do dia 26 de junho de 2007, registrou-se uma média de 141,1354 mensagens a cada 15 minutos, com desvio-padrão de 152,3156 e coeficiente de variação de 1,0792. Esse comportamento é típico ao longo de todo o tráfego estudado, onde o menor coeficiente de variação registrado foi 0,5399. Esse comportamento também não é surpreendente, uma vez que o número de eventos que ocorrem na rede e que causam emissão de `traps` pode perfeitamente variar bastante ao longo de um dia na rede.

`response`

As mensagens `response` são observadas na rede gerenciada sempre em resposta a mensagens `get-request`, `get-next-request` e `get-bulk-request`, contendo as informações dos objetos requisitados pelo gerente. Devido a essa característica, é esperado que as mensagens `response` possuam comportamento bastante semelhante ao da união das mensagens `get-request`, `get-next-request` e `get-bulk-request`. De fato, observou-se, no caso específico da rede da RNP, que, conforme esperado, a distribuição da quantidade de mensagens `response` apresentava componentes periódicos e aperiódicos. Esse comportamento pode ser observado na Figura 7 abaixo.

Na distribuição representada na Figura 7, a média registrada foi de 12.398,66 mensagens a cada 15 minutos, com desvio padrão de 55,33 e coeficiente de variação de 0,0045. Esse dado nos mostra que, apesar da existência de componentes aperiódicos, a quantidade de mensagens do tipo `response` tem uma distribuição bastante constante e periódica no geral (conforme observa-se na maioria absoluta da representação da distribuição das mensagens), de modo similar àquela representada na Figura 2 referente à distribuição de mensagens `get-request`. Esse comportamento também se repete em todos os dias onde houve monitoramento do tráfego SNMP da RNP.

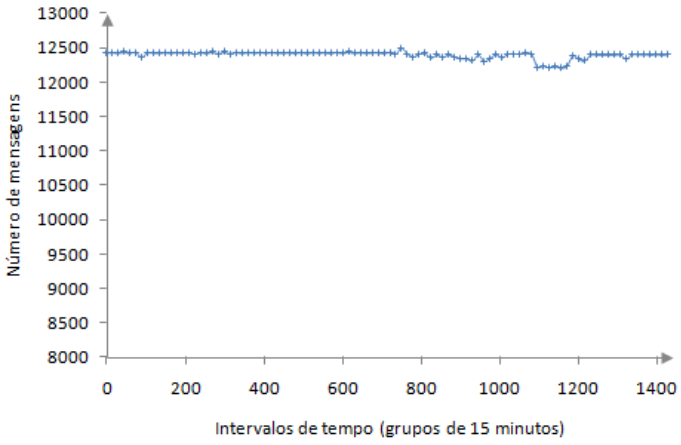


Figura 7. Distribuição do número de mensagens response amostrada em intervalos de 15 minutos, observada no dia 3 de julho de 2007

4.4. Correlações verificadas no tráfego SNMP da rede da RNP

Uma vez que a maioria das mensagens do SNMP atendem a eventos específicos e independentes entre si, espera-se que existam poucas correlações entre as distribuições dos diversos tipos de mensagens que compõem o protocolo. As mensagens com maior potencial de correlação são as do tipo `get` (i.e., `get-request`, `get-next-request` e `get-bulk-request`) com as suas respectivas mensagens de `response`.

Na análise de cada um dos dias do tráfego de gerenciamento da RNP em que houve monitoramento, percebeu-se que os maiores coeficientes de correlação encontravam-se entre as mensagens `get-request` e `response` (correlação tipicamente variando entre 0,80 e 0,90 para cada um dos dias observados). Esse fato se explica porque a maior parte do *polling* realizado na rede é feito com o uso de mensagens `get-request`,e para cada uma dessas mensagens uma mensagem `response` é gerada. Além disso, a operação `get-request`, juntamente com seus respectivos `responses`, praticamente dominam o tráfego periódico na rede gerenciamento da RNP, o que contribui para que a correlação entre eles seja alta.

As demais mensagens observadas ao longo do tráfego monitorado possuem baixa correlação. Tipicamente, o coeficiente de correlação entre essas mensagens varia de 0 a 0,25.

5. Conclusões e trabalhos futuros

A partir das análises realizadas sobre o tráfego fornecido pela Rede Nacional de Ensino e Pesquisa (RNP), foi possível se chegar a um conjunto de resultados interessantes acerca do protocolo SNMP. Atualmente, existe um grande esforço por parte da comunidade de pesquisa em gerenciamento e operação de redes de computadores para se determinar os padrões de uso do protocolo SNMP nas redes em produção. O presente estudo contribui com esse esforço, através de dados que ora confirmam vários dos aspectos que eram apenas pressupostos sobre o uso do SNMP, ora trazem a tona novas características ainda desconhecidas pela comunidade de gerenciamento de redes. Muitas das análises que foram empregadas neste trabalho não haviam sido utilizadas anteriormente em outros trabalhos inseridos no contexto da caracterização do uso do protocolo SNMP. Em

especial, as análises das distribuições dos números de mensagens em perspectiva com a dimensão temporal do tráfego monitorado demonstrou ser capaz de fornecer *insights* bastante interessantes acerca do comportamento do protocolo SNMP na rede da RNP, tais como: identificação de componentes aperiódicos em momentos específicos do tráfego monitorado, níveis de variação tipicamente relacionados com cada operação do protocolo SNMP, potencial para otimização do tráfego de *polling* a partir de modificações nas operações utilizadas para recuperação de valores dos agentes da rede, entre outros.

O tráfego SNMP estudado se mostrou, predominantemente, constante e periódico. Esse comportamento já era esperado, uma vez que a maior parte das ferramentas de gerenciamento de redes conhecidas faz uso extenso de *polling* para determinar o estado dos vários agentes que estão sendo gerenciados. Seria desejável o estudo do comportamento da geração de mensagens feita pelas ferramentas de gerenciamento da rede, a fim de melhor explicar os fenômenos aqui estudados. Contudo, esse tipo de análise não é factível, uma vez que os dados das mensagens contidas na amostra de tráfego SNMP não são suficientes para que "porções" de tráfego provenientes de ferramentas de gerenciamento distintas sejam isoladas.

Foi possível também se identificar um componente aperiódico nesse mesmo tráfego, inclusive criado a partir de mensagens que são tipicamente usadas para a execução do *polling* na rede, como é o caso do `get-request`. Esse componente é significativo o suficiente para justificar um estudo mais aprofundado do mesmo, sendo necessário isolá-lo da parte periódica do tráfego, a fim de ser melhor analisado. Os autores do presente artigo planejam a realização de um estudo desse tipo para o futuro.

Os recursos do SNMP para notificação (`traps`) se mostraram pouco utilizados na rede estudada, em detrimento do extenso uso de *polling*. Ressalta-se que o uso de traps é recomendado no SNMP a fim de diminuir a sobrecarga de mensagens de gerenciamento sobre a rede. Os coeficientes de variação do número de mensagens do tipo `trap` foram os maiores dentre os analisados no tráfego SNMP da RNP, fato este que não representou uma surpresa para os autores deste trabalho.

Conforme esperado, observou-se que o SNMP é utilizado na rede da RNP exclusivamente para monitoramento dos dispositivos e serviços, e nunca para configuração dos mesmos. Isso provavelmente se deve aos problemas de segurança que o SNMP pode apresentar para configuração de recursos na rede, uma vez que as *strings* de comunidade, que funcionam como uma espécie de senha nesse tipo de operação, trafegariam em claro na rede. A possibilidade de criptografar esse tipo de informação só surgiu a partir da versão 3 do SNMP; este, porém, ainda não é suportado por vários dos dispositivos de rede atuais. Também por esse motivo não foram registradas no tráfego da RNP mensagens da versão 3 do SNMP.

Referências

Androutsellis-Theotokis, S. and Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Comput. Surv.*, 36(4):335–371.

Case, J. D., Fedor, M. L., and Schoffstal, J. D. (1990). Simple Network Management Protocol (SNMP). RFC 1157. [S.l.]: Internet Engineering Task Force, Network Working Group.

Curbera, F., Duftler, M., Khalaf, R., Nagy, W., Mukhi, N., and Weerawarana, S. (2002). Unraveling the web services web - an introdution to soap, wsdl,and uddi. *IEEE Internet Computing*, 6(2):86–93.

Dobrev, P., Stancu-Mara, S., and Schönwälder, J. (2009). Visualization of node interaction dynamics in network traces. In *AIMS '09: Proceedings of the 3rd International Conference on Autonomous Infrastructure, Management and Security*, pages 147–160, Berlin, Heidelberg. Springer-Verlag.

Goldszmidt, G. and Yemini, Y. (1995). Distributed management by delegation. In *Proceedings of the 15th International Conference on Distributed Computing Systems, 1995*, pages 333–340, Vancouver, BC, Canada.

Salvador, E. M. and Granville, L. Z. (2008a). Arquitetura de uma ferramenta e técnicas de visualização para medições sobre tráfego snmp. In *Simpósio Brasileiro de Redes de Computadores, SBRC, 26.*, Rio de Janeiro, Brasil.

Salvador, E. M. and Granville, L. Z. (2008b). Using visualization techniques for snmp traffic analyses. In *IEEE Symposium on Computers and Communications, ISCC*, Marrakesh, Marrocos.

Schönwälder, J., Pras, A., Harvan, M., Schippers, J., and van de Meent, R. (2007). SNMP Traffic Analysis: Approaches, Tools, and First Results. *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management*.

Schoenwaelder, J. (2008). Simple Network Management Protocol (SNMP) Measurements and Trace Exchange Formats. *Internet Research Task Force (IRTF), RFC 5345*.

Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., and Waldbusser, S. (2001). Rfc 3198 - terminology for policy-based management. Disponível em `ftp://ftp.rfc-editor.org/in-notes/rfc3198.txt`. Acesso em maio de 2006.

Análise de Uso e Mobilidade em uma Rede sem Fio Urbana de Larga Escala

Fernanda Vilas Boas Fuscaldi[1], **Cristina Duarte Murta**[1]

[1]Departamento de Computação — CEFET–MG
Belo Horizonte, MG

cristina@decom.cefetmg.br

Resumo. *Redes sem fio de larga escala estão sendo implantadas em grandes áreas urbanas. Este artigo apresenta uma análise do uso de uma rede sem fio urbana de larga escala e acesso público e gratuito, implantada na cidade de Montreal, Canadá. Os dados de acesso à rede foram coletados continuamente, durante um período de três anos. Os aspectos analisados incluem a evolução do uso da rede, caracterização de tráfego, perfis de usuários e padrões de mobilidade. Os resultados são importantes para o planejamento de redes sem fio urbanas de larga escala, bem como para a geração de modelos de carga para experimentos e simulação.*

Abstract. *Wireless networks have being widely deployed in large urban areas. This paper presents an analysis of usage data collected of a large-scale free public access wireless network deployed in the city of Montreal, Canada. The network access data were collected continuously for a period of three years. Some aspects discussed include the evolution of the network usage, traffic characterization, user profiles and mobility patterns. These results are important for the planning of large-scale wireless networks, as well as for the generation of accurate workload models for experiments and simulation.*

1. Introdução

Redes sem fio urbanas de larga escala e acesso gratuito estão pouco a pouco tornando-se realidade nos grandes centros. Encontradas frequentemente em instituições, empresas e escolas, as redes sem fio estão surgindo em grandes áreas públicas, tendo como foco uma região geográfica maior, como o centro de uma grande cidade. Montreal, San Francisco, New York, Adelaide, Orlando e Austin são exemplos de cidades que já implantaram redes sem fio extensas. Projetos similares estão sendo implantados em cidades brasileiras como, por exemplo, em Belo Horizonte [BH Digital 2009].

Mobilidade e flexibilidade são duas características inerentes às redes sem fio. Em conjunto com dispositivos de mão que permitem conexão à Internet, estas redes contribuem para facilitar o acesso a Internet a partir de qualquer lugar. A possibilidade de acessar aplicações e serviços na Web independentemente do tipo de rede de acesso e da mobilidade do usuário encontra desafios tais como heterogeneidade dos dispositivos de acesso, ambientes híbridos, problemas de desempenho, além de questões econômicas relacionadas a tarifação e contabilização de uso.

A caracterização do uso, da mobilidade e da experiência do usuário provê informações importantes para o projeto e o dimensionamento das redes, bem como para

a análise e previsão de desempenho de programas e aplicações destinadas a ambientes móveis. Além disso, a caracterização e análise dos dados são fundamentais para a geração de modelos que podem ser usados em ferramentas de simulação que incluem modelos de mobilidade, resultando em redes sem fio mais confiáveis.

Diversos estudos têm sido publicados descrevendo características de acesso e de uso de redes sem fio públicas e privadas. No entanto, a maioria dos estudos trata de redes em ambientes relativamente pequenos, como residências [Papagiannaki et al. 2006], centros de pesquisa [Balazinska and Castro 2003, Tang and Baker 2000] ou ambientes acadêmicos limitados a um campus [Campos and Papadopoull 2005]. Caracterizações de redes maiores são recentes [Brik et al. 2008, Afanasyev et al. 2008]. Independentemente do alcance da rede, todos estes trabalhos apresentam o estudo da rede em um período curto, o que não permite a análise da evolução do uso da rede.

Este artigo apresenta uma caracterização e análise do tráfego e do uso da rede sem fio denominada *Île Sans Fil* [Île Sans Fil 2008], implantada na cidade de Montreal, Canadá. O objetivo deste trabalho é investigar o tráfego e o uso de uma rede sem fio em uma grande área urbana. Dados de uso da rede foram coletados de forma contínua durante um período de três anos, o que permite um estudo da evolução do uso da rede neste período. Este artigo se distingue dos demais pelo fato de analisar a evolução do uso de uma rede grande, urbana, de acesso público e gratuito, em período longo. Quanto ao nosso conhecimento, este é o primeiro artigo que analisa o uso de uma rede com estas características.

A disponibilidade de informações sobre o uso de uma rede grande, comunitária e de acesso gratuito, durante um tempo tão longo é uma oportunidade ímpar para um estudo de evolução do uso do sistema. Entre as questões de interesse estão como e quando as pessoas usam a rede, qual foi o crescimento do número de usuários e do tráfego na rede no período, quais são as principais características da mobilidade dos usuários e a distribuição da carga nos pontos de acesso.

As principais conclusões do artigo são as seguintes. A maior parte dos usuários utilizou a rede apenas uma vez. No entanto, observa-se uma fração significativa de usuários muito frequentes e com alta mobilidade. A distribuição da carga na rede é desigual, uma fração pequena de pontos de acesso responde pela maior parte da carga. O crescimento do número de usuários e do número de acessos foi expressivo durante o período. No entanto, não houve aumento na duração da sessão. Os usuários utilizam a rede predominantemente no período diurno.

O conhecimento resultante deste trabalho pode ser aplicado no planejamento e dimensionamento de outras redes sem fio de porte similar, e em pesquisa na área de redes sem fio. Por exemplo, a caracterização da diversidade dos usuários em termos de uso da rede e da mobilidade oferece oportunidades para novas propostas de escalonamento e comunicações oportunistas.

Este artigo está organizado em cinco seções. A Seção seguinte discute os trabalhos relacionados. A Seção 3 apresenta a descrição da rede e da informação disponível para análise. A Seção 4 apresenta os resultados e a Seção 5 conclui o trabalho.

Tabela 1. Algumas redes sem fio analisadas na literatura

Rede	Hotspots	Período	Cobertura	Uso	Ambiente
RoofNet	38	horas	6 km^2	teste	urbano
UNC	232	2 meses	3 km^2	não comercial	campus
TFA@Rice	18	minutos	4 km^2	não comercial	urbano
MadMesh	224	2 semanas	26 km^2	comercial	urbano
Google WiFi	500	28 dias	31 km^2	misto	urbano
Île Sans Fil (este artigo)	206	3 anos	16 km^2	não comercial	urbano

2. Trabalhos Relacionados

Há numerosos trabalhos relacionados à caracterização e análise de redes sem fio. A Tabela 1 compara algumas redes analisadas na literatura. A rede experimental RoofNet [Aguayo et al. 2004] instalada pelo MIT na cidade de Cambridge, MA, foi objeto de um experimento cujo objetivo foi analisar padrões de perdas de pacotes, em particular, investigar a importância relativa das perdas e das interações entre perdas no desempenho geral da rede, e suas implicações no projeto de protocolos de roteamento.

Uma análise de mobilidade e padrões de acesso observados na rede sem fio UNC instalada em um campus é apresentada em [Campos and Papadopoull 2005]. O artigo propõe também uma metodologia para caracterizar acessos a redes sem fio baseadas em visitas e sessões. Os resultados são fortemente associados aos horários das atividades na instituição e à disposição e distância entre os prédios do campus. A relação entre maior mobilidade e menor duração da visita a um *site* do campus é apontada no artigo.

Redes maiores são analisadas em artigos mais recentes [Camp et al. 2006, Brik et al. 2008, Afanasyev et al. 2008]. O primeiro artigo [Camp et al. 2006] analisa a rede urbana TFA@Rice implantada na cidade de Houston, TX, particularmente em relação ao ambiente de propagação, perdas e *throughput*. A análise dos experimentos indica que o conhecimento detalhado do ambiente de propagação e da relação entre o sinal e o *throughput* são críticos para a implantação da rede. A rede comercial MadMesh, descrita em [Brik et al. 2008], está instalada na cidade de Madison, WI. Os objetivos daquele estudo foram analisar a eficácia das estratégias de implantação da rede, a experiência do usuário em relação ao desempenho observado e as características de uso da rede. A rede Google WiFi, discutida em [Afanasyev et al. 2008], está instalada na cidade de Mountain View, CA, e é uma rede de uso misto (comercial e não comercial) com taxa de transmissão limitada a 1Mb/s para clientes individuais. Os objetivos daquele estudo foram caracterizar o acesso temporal dos usuários, suas demandas de tráfego e sua mobilidade na rede. Três tipos de usuários foram identificados, e cada tipo apresentou características distintas em relação aos aspectos estudados.

Modelos de mobilidade tem grande efeito nos resultados de simulação e podem afetar de forma significativa os resultados de estudos de desempenho da rede [Hong et al. 2001]. Uma proposta para caracterização da mobilidade é apresentada em [Campos and de Moraes 2007]. Uma análise da trajetória de cem mil usuários de telefone celular é feita em [Gonzalez et al. 2008]. As conclusões indicam que as trajetórias humanas apresentam alto grau de correlação temporal e espacial e seguem padrões simples e de fácil reprodução.

3. Descrição da Rede e Informação Coletada

Île Sans Fil [Île Sans Fil 2008] é uma organização sem fins lucrativos que oferece em Montreal, Canadá, acesso gratuito à Internet para a comunidade via rede Wi-Fi (padrão IEEE 802.11). Os objetivos da organização são oferecer recursos tecnológicos para as pessoas, promover o trabalho comunitário, além de fortalecer a comunidade local. Em 2007, a organização tornou disponível para a comunidade acadêmica os registros de acesso à rede feitos em um período de três anos, de 2004 a 2007 [CRAWDAD 2008]. A Tabela 2 apresenta os principais números da rede: dados de acesso foram coletados durante exatos 1096 dias, iniciados em 27 de agosto de 2004 e finalizados em 27 de agosto de 2007. Neste período, todos os acessos feitos foram registrados. Quase setenta mil usuários distintos utilizaram a rede no período, realizando mais de 580.000 sessões por meio de 206 pontos de acesso.

Tabela 2. Números Coletados da Rede

Número de sessões	587.780
Usuários únicos	69.689
Número de estações	206
Placas de rede	43.791
Número de dias	1.096

Os dados foram coletados por um software projetado e implementado para auxiliar a operação da rede, denominado WifiDog [Île Sans Fil 2008]. Embora o acesso seja gratuito, os usuários devem registrar-se para acessar a rede. Os dados coletados pelo WifiDog foram registrados por sessão do usuário, definida como o tempo entre o início e o fim da conexão. Cada sessão recebeu um número de identificação, seguido da identificação do usuário, identificação do ponto de acesso (*hotspot*), identificação da placa de rede (MAC *address*), dia e hora de início da sessão, dia e hora de fim da sessão, número de bytes recebidos e número de bytes enviados. Os dados relativos ao usuário, endereço de rede, identificação da conexão e do ponto de acesso foram anonimizados [CRAWDAD 2008]. Os campos de cada registro são apresentados na Tabela 3.

Tabela 3. Definição dos Dados Coletados

Campo	Significado
conn_id	Identificação da conexão
timestamp_in	Tempo de início da sessão
node_id	Identificação do ponto de acesso
timestamp_out	Tempo de fim da sessão
user_id	Identificação do usuário
user_mac	Endereço MAC
incoming	Quantidade de dados recebida (Bytes)
outgoing	Quantidade de dados transferida (Bytes)

Um mapa dos pontos de acesso é apresentado na Figura 1. Cada balão representa um ponto de acesso à rede. As setas internas indicam se o ponto de acesso estava operacional (seta para cima) ou não, no momento da captura da imagem. A rede cobre uma área

de 16 km^2, com pontos de acesso agrupados em uma linha de 8 km na direção norte–sul e 5 km na direção leste–oeste [Crow and Miller 2008].

Figura 1. Localização dos pontos de acesso da rede na cidade de Montreal [Île Sans Fil 2008].

4. Resultados

Nesta seção são apresentados os resultados da caracterização e análise dos registros de acesso à rede Île Sans Fil durante o período de três anos. Inicialmente, o crescimento do uso da rede no período é analisado. A seguir, é apresentada a caracterização das sessões realizadas pelos usuários no período, incluindo o número e a duração das sessões, bem como o tráfego gerado. O perfil do usuário, incluindo a caracterização de mobilidade, é descrito na última subseção.

4.1. Crescimento da Rede no Período

A Figura 2 apresenta dados do crescimento do uso da rede ao longo do período de 1096 dias. O gráfico à esquerda indica o registro de novos usuários. O gráfico no centro da Figura indica o crescimento do número de sessões registradas por dia. O crescimento do número de novos usuários e de sessões no período pode ser modelado por uma função quadrática. O gráfico à direita apresenta a data da primeira ocorrência de cada ponto de acesso nos registros. Este gráfico indica que a infraestrutura da rede também cresceu no período e o crescimento foi linear em relação ao tempo: ao final do primeiro ano havia cerca de 70 pontos de acesso, número que chegou a 140 ao final do segundo ano e 206 ao completar o terceiro ano.

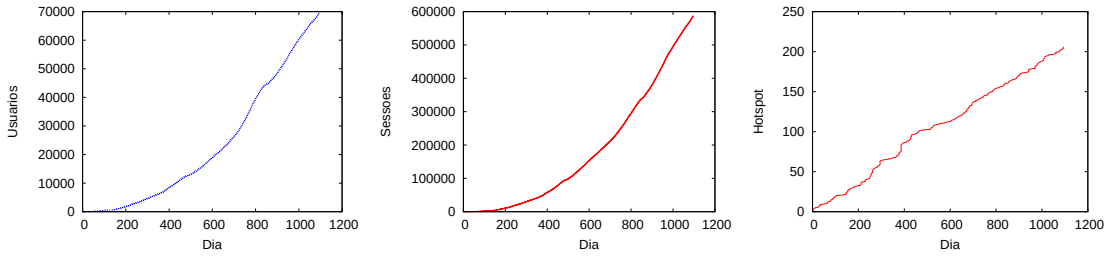


Figura 2. Crescimento do número de usuários, sessões e pontos de acesso ao longo do período.

4.2. Uso da Rede no Período

A seguir analisamos a duração das sessões e a quantidade de bytes transferida em todas as sessões ocorridas no período. A Figura 3 apresenta as curvas PDF e CDF da duração das sessões. Observa-se que 50% das sessões tem duração inferior a 35 minutos e 90% das sessões tem duração inferior a duas horas e 42 minutos. No entanto, há sessões com duração de mais de vinte horas.

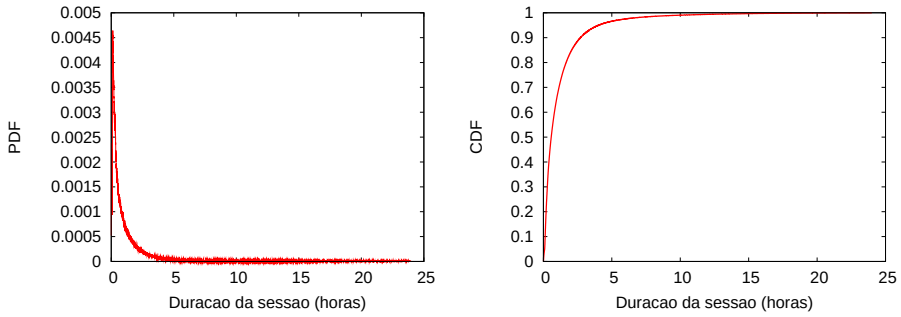


Figura 3. Duração da sessão.

A Figura 4 apresenta os resultados do tráfego gerado pelas sessões. O gráfico à esquerda da Figura apresenta as curvas de frequência acumulada da quantidade de bytes recebida e enviada em cada sessão. Os dados indicam que a quantidade de bytes enviada é inferior à quantidade de bytes recebida em cada sessão, em média. A relação entre a duração da sessão e a quantidade de bytes recebida pode ser analisada no gráfico à direita da mesma Figura. Os pontos apresentam uma correlação no limite inferior do conjunto, indicando que quantidades maiores de bytes são transmitidas em sessões mais longas. No entanto, observamos também que sessões curtas podem transmitir quantidades significativas de dados (em bytes). Um padrão similar foi observado em [Afanasyev et al. 2008].

A Figura 5 apresenta dados do crescimento do uso da rede ao longo dos três anos de acesso. O gráfico à esquerda apresenta o número de sessões registrado a cada dia. Há três quedas significativas no número de sessões, próximas aos dias 120, 485 e 850, que correspondem ao dia de Natal de cada ano. O gráfico no centro apresenta dados do número médio de bytes recebidos por sessão, para todas as sessões de um dia. O gráfico à direita apresenta a duração média das sessões, obtendo-se a média para todas as sessões de um dia. Os gráficos indicam um crescimento expressivo do uso da rede no período quanto ao número de sessões e bytes transmitidos por sessão, mas não na duração da sessão. O número de sessões por dia aumentou de cerca de 100 no primeiro ano para

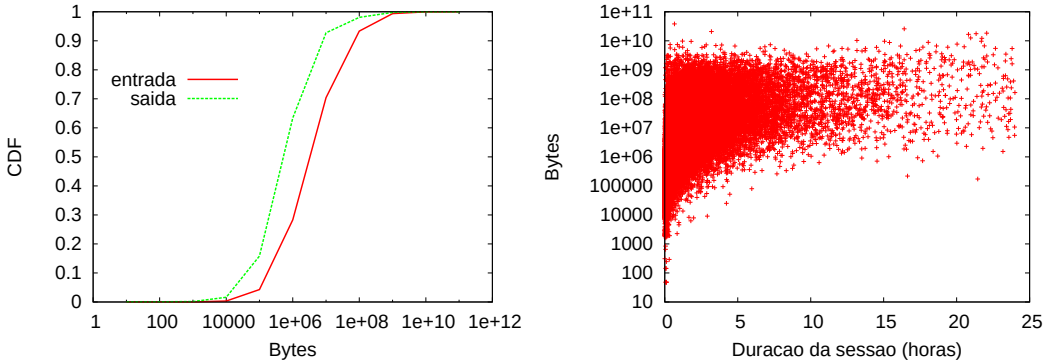


Figura 4. Quantidade de bytes recebida e enviada por sessão (esq.) e bytes transferidos em função da duração da sessão (dir.).

1000 sessões por dia no terceiro ano. O número de bytes recebidos em média por sessão passou de unidades de megabytes para centenas de megabytes. A duração média da sessão manteve-se praticamente estável no período, em torno de 4246 segundos, i.é, uma hora e dez minutos.

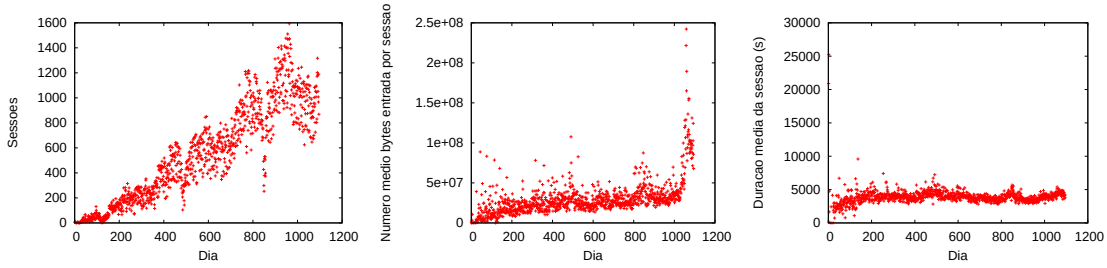


Figura 5. Evolução do acesso à rede ao longo do período.

A Figura 6 apresenta o número de usuários ativos a cada hora do dia, ao longo de um período de vinte e oito dias escolhido aleatoriamente. Observamos um padrão de acesso relacionado à hora do dia, com maior atividade para o período diurno. Há também um padrão semanal, com menor acesso nos fins de semana. O uso da rede ao longo do dia é apresentado na Figura 7. Observamos que a maior parte dos acessos é feita nos horários diurnos, com pico em torno das 15 horas (horário local).

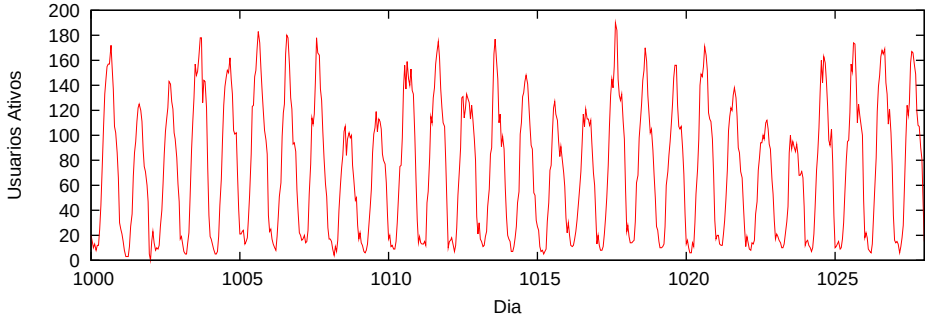


Figura 6. Número de usuários ativos ao longo de 28 dias.

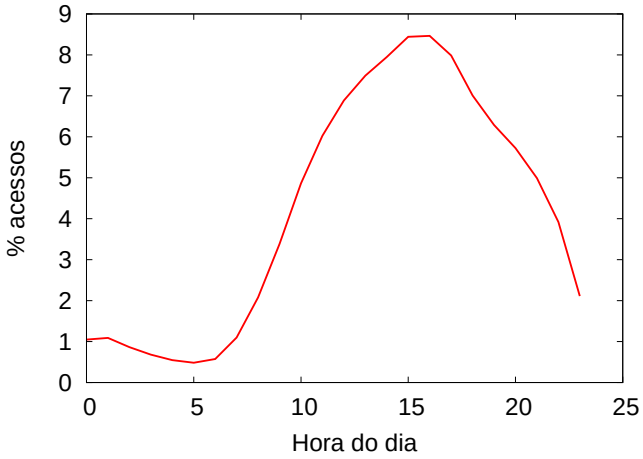


Figura 7. Frequência média de acesso por hora do dia.

4.3. Perfil do Uso da Rede por Usuário e Mobilidade

Esta seção focaliza o perfil dos usuários quanto ao uso da rede e sua mobilidade. O perfil de uso refere-se à frequência de acesso à rede no período analisado. A mobilidade é analisada relacionando a sessão do usuário ao ponto de acesso registrado para cada sessão feita.

A Figura 8 apresenta dois gráficos. O gráfico à esquerda mostra a curva CDF do número de sessões realizadas por usuário. Observamos que a maioria dos usuários (63%) utilizou a rede somente uma vez (*one-time users*). Este é um valor alto comparado com outros estudos. Por exemplo, na rede Google WiFi, 35% dos usuários fizeram apenas uma conexão ao sistema [Afanasyev et al. 2008]. Esta diferença pode ser explicada pelo fato de que a rede Google WiFi é uma rede com apelo comercial, o que indica interesses diferentes por parte dos usuários quanto ao uso da rede. A rede *Île Sans Fil* é uma rede de acesso público e gratuito, para a população em geral. Além disso, o intervalo de tempo analisado no nosso caso é muito maior (vide Tabela 1) e entendemos que o número de *one-time users* aumenta com o tempo de coleta de dados, para sistemas em implantação, como é o caso destas duas redes. Ainda no mesmo gráfico (à esquerda da Figura 8) observamos que uma pequena fração de usuários utiliza intensamente a rede. O eixo x está em escala logarítmica.

O gráfico à direita da Figura 8 apresenta a curva CDF do número de pontos de acesso utilizado pelos usuários em suas sessões. Além dos 63% de usuários que utilizaram a rede apenas uma vez e, portanto, utilizaram somente um ponto de acesso, 20% dos usuários utilizaram a rede mais de uma vez mas sempre a partir do mesmo ponto de acesso. Portanto, 11.311 usuários (17%) utilizaram mais de um ponto de acesso e estes são os usuários móveis, do ponto de vista deste estudo.

A relação entre o número de sessões realizadas pelos usuários móveis e o número de pontos de acesso utilizados para estas sessões é mostrada na Figura 9. O gráfico indica que há usuários muito frequentes que utilizam poucos pontos de acesso, dois a cinco, por exemplo, e há usuários frequentes que utilizaram muitos pontos de acesso.

A mobilidade de alguns usuários é representada na Figura 10. A mobilidade é

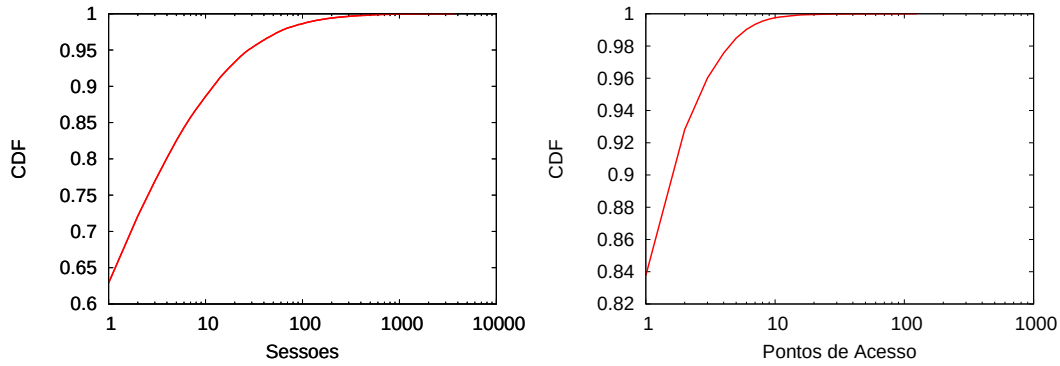


Figura 8. Número de sessões por usuário (esq.) e número de pontos de acesso utilizados por usuário (dir.) durante o período analisado.

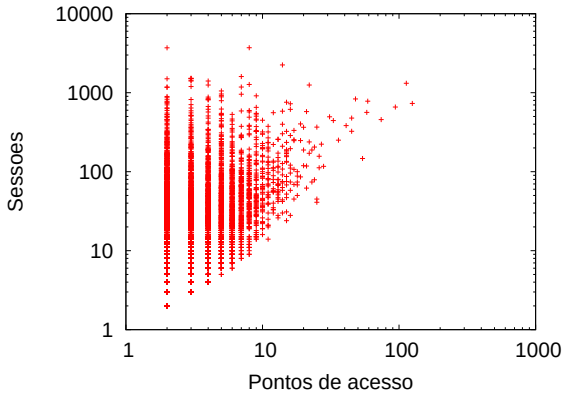


Figura 9. Número de sessões e pontos de acesso utilizados por usuários frequentes.

analisada em termos da realização de sessões consecutivas no mesmo ponto de acesso ou em um ponto de acesso distinto. Entre os usuários móveis, selecionamos os 5% que apresentaram maior mobilidade e analisamos a frequência de mudança de ponto de acesso para sessões consecutivas. A análise indica que 54% dos acessos destes usuários foi feito no mesmo ponto de acesso da sessão anterior, e em 46% dos casos os acessos foram feitos a partir de um ponto de acesso diferente.

Para avaliar a carga nos pontos de acesso, contamos a frequência de acessos em cada ponto de acesso, que é mostrada no gráfico à esquerda da Figura 11. O gráfico à direita da mesma Figura apresenta a frequência acumulada, considerando os pontos de acesso ordenados do mais utilizado para o menos utilizado. Observamos que 20 pontos de acesso (aproximadamente 10%) são responsáveis por 50% do uso da rede, e 85 (cerca de 41%) recebem 90% da carga.

5. Conclusões

Este artigo apresentou uma caracterização do acesso à rede sem fio *Île Sans Fil*, considerada a melhor rede sem fio canadense em vários aspectos [Crow and Miller 2008]. Todos os dados coletados foram analisados. A rede tem foco comunitário e isso parece refletir no seu uso, sendo, portanto, difícil comparar os resultados com outras análises de redes sem fio instaladas em universidades e instituições ou redes comerciais. No entanto, é razoável

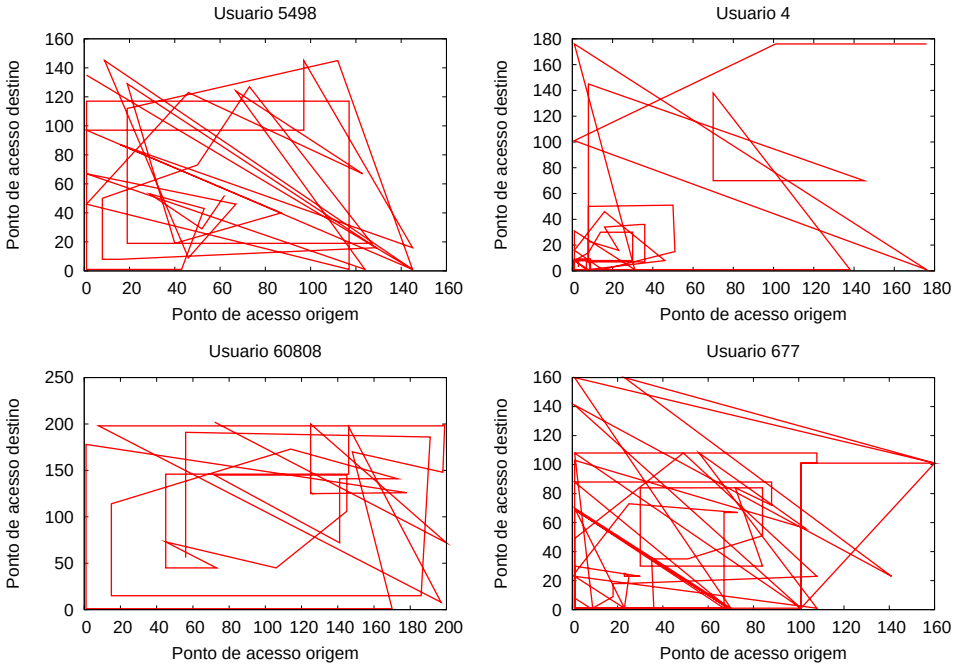


Figura 10. Mobilidade de alguns usuários: linhas representam sessões consecutivas feitas a partir de pontos de acesso diferentes.

esperar que redes sem fio com este foco sejam implantadas amplamente em várias cidades do mundo. Neste sentido, este artigo contribui com informações importantes para o projeto e o dimensionamento de redes similares. Além disso, as informações podem ser utilizadas em simulações e análises de desempenho. A análise da mobilidade a partir da localização física de cada ponto de acesso e das distâncias entre eles é uma possibilidade de trabalho futuro com o objetivo de propor um modelo de mobilidade a partir dos dados reais coletados.

Agradecimentos

Agradecemos às equipes do CRAWDAD e da *Île Sans Fil* por tornarem disponíveis os dados de acesso à rede, sem os quais este trabalho não seria possível. Este trabalho foi parcialmente financiado pelo CNPq e pela FAPEMIG.

Referências

Afanasyev, M., Chen, T., Voelker, G. M., and Snoeren, A. C. (2008). Analysis of a Mixed-Use Urban WiFi Network: When Metropolitan becomes Neapolitan. In *Internet Measurement Conference*, San Diego,USA.

Aguayo, D., Bicket, J., Sanjit Biswas, G. J., and Morris, R. (2004). Link-level Measurements from an 802.11b Mesh Network. In *ACM SIGCOMM*.

Balazinska, M. and Castro, P. (2003). Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network. In *1st International Conference on Mobile Systems, Applications, and Services (MobiSys)*, San Francisco, CA.

BH Digital (2009). BH Digital. http://blog.mg.gov.br/bh-digital-implanta-espacos-gratuitos-de-acesso-a-internet.

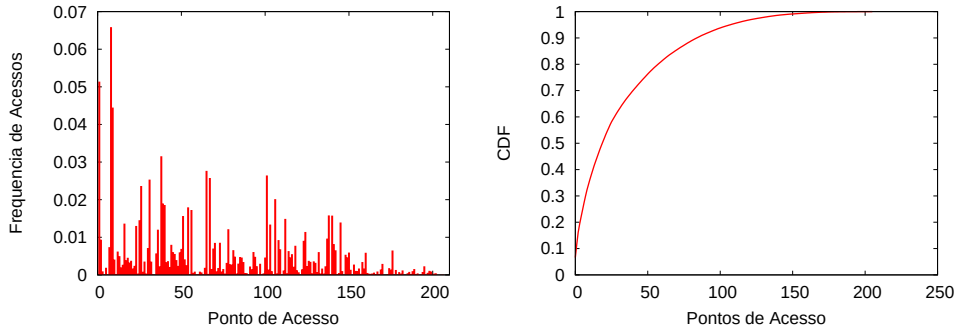


Figura 11. Frequência de uso de cada ponto de acesso (esq.) e frequência acumulada do uso dos pontos de acesso (dir.)

Brik, V., Rayanchu, S., Saha, S., Sen, S., Shrivastava, V., and Banerjee, S. (2008). A Measurement Study of a Commercial-grade Urban WiFi Mesh. In *Internet Measurement Conference*, Madison,USA.

Camp, J., Robinson, J., Steger, C., and Knightly, E. (2006). Measurement driven deployment of two-tier urban mesh access network. In *ACM MobiSys*.

Campos, C. A. V. and de Moraes, L. F. M. (2007). Uma Proposta de Caracterização da Mobilidade de Usuários Sem Fio Através de Medição Real. In *XXV Simpósio Brasileiro de Telecomunicações*.

Campos, F. H. and Papadopoull, M. (2005). A Comparative Measurement Study of the Workload of Wireless Access Points in Campus Networks. In *IEEE International Symposium on Personal Indoor and Mobile Radio Communications*, volume 3, pages 1776–1780.

CRAWDAD (2008). Community Resource for Archiving Wireless Data At Dartmouth. http://crawdad.cs.dartmouth.edu.

Crow, B. and Miller, T. (2008). Community Wireless Infrastructure Research Project: Île Sans Fil Case Study Map. http://www.cwirp.org/.

Gonzalez, M., Hidalgo, C., and Barabasi, A.-L. (2008). Understanding Individual Human Mobility Patterns. *Nature*, pages 779–782.

Hong, X., Kwon, T. J., Gerla, M., Gu, D. L., and Pei, G. (2001). A Mobility Framework for Ad Hoc Wireless Networks. In *MDM '01: Proceedings of the Second International Conference on Mobile Data Management*, pages 185–196, London, UK. Springer-Verlag.

Île Sans Fil (2008). http://www.ilesansfil.org.

Papagiannaki, K., Yarvis, M., and Conner, S. W. (2006). Experimental Characterization of Home Wireless Networks and Design Implications. In *Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM)*, Barcelona, Spain.

Tang, D. and Baker, M. (2000). Analysis of a Local-area Wireless Network. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 1–10, New York, NY, USA. ACM.

Monitoração de qualidade de serviço de redes com aplicações de tempo-real utilizando técnicas de amostragem baseadas em CEP

Renata M. S. Wowk[1], Edgard Jamhour[1]

[1]PPGIA – Pontifícia Universidade Católica do Paraná (PUCPR)
CEP 80215-901 – Curitiba – PR – Brazil

renata@softall.com.br, jamhour@ppgia.pucpr.br

Resumo. *Aplicações em tempo real como "Voz sobre IP" (VoIP) demandam monitoração de métricas de qualidade, de forma a garantir que os serviços sejam atendidos adequadamente e, em caso de problema, permitam uma rápida identificação do ponto onde a métrica não está de acordo com os níveis delineados. Este trabalho propõe um algoritmo que permite monitorar o desempenho de uma rede em longos períodos de operação, através de um processo de amostragem dinâmico, capaz de identificar os momentos que ocorrem alterações significativas no comportamento da rede. Este algoritmo é baseado em técnicas de controle estatístico de processos (CEP). O algoritmo proposto foi avaliado em ambiente de laboratório, onde o desempenho do transporte do tráfego VoIP em uma rede sujeita a congestionamento foi monitorado através da métrica MDI (Media Delivery Index).*

1. Introdução

A convergência de voz e dados em uma mesma infra-estrutura de rede requer garantia de níveis de qualidade adequados para as aplicações sensíveis a atraso, como voz sobre IP (VoIP). Por este motivo, no momento da contratação do serviço de uma operadora de telecomunicações devem-se definir os requisitos do serviço, os mecanismos para sua medição e os processos que definem a aplicação de multas e recompensas quando os níveis atingidos não forem os acordados. Considerando o alto volume de tráfego nas redes atuais, são necessárias técnicas de medições de tráfego baseadas em amostragem para monitorar os níveis de serviço, pois se o volume de dados coletados para avaliar o desempenho da rede for muito grande, o custo dos equipamentos de monitoramento será elevado e a análise dos dados pode tornar-se inviável.

Este trabalho propõe um algoritmo que permite monitorar o desempenho de uma rede por longos períodos de operação, através de um processo de amostragem dinâmico, capaz de identificar os momentos que ocorrem alterações significativas no comportamento da rede. A aplicação deste algoritmo pode servir como base para validação de acordos de nível de serviço (SLA). A ênfase especial foi para monitoração de métricas que registrem o comportamento de aplicações em tempo real, pois estas precisam ser registradas continuamente durante a operação da rede. A técnica de amostragem utilizada pode ser utilizada para acompanhamento de diversos parâmetros de desempenho da rede, como atraso, perda de pacotes e variabilidade de atraso (jitter). Contudo, esse trabalho enfatizou o uso de uma nova métrica, denominada Media

Delivery Index – MDI , o qual será explicada neste trabalho. Ressalta-se que, embora a proposta do MDI tenha ênfase no cálculo da métrica para pacotes MPEG, a metodologia pode ser utilizada em outras aplicações que sejam sensíveis a atraso ou jitter, como por exemplo, VoIP.

O algoritmo proposto utiliza o método estatístico denominado CEP (Controle Estatístico de Processo) para registro contínuo do desempenho da rede durante longos períodos de tempo. A técnica de CEP permite detectar mudanças significativas em um processo, diferenciando oscilações aleatórias das verdadeiras mudanças de tendência um processo [MONTGOMERY, 2005]. A técnica de CEP é bastante comum na indústria de manufatura, mas ao nosso conhecimento, raramente utilizado na modelagem de redes de comunicação como processos, o que consiste em uma abordagem inovadora desse trabalho. Neste trabalho a técnica de CEP é utilizada para controlar a taxa de amostragem de pacotes de acordo com o comportamento do desempenho da rede. Se o desempenho da rede estiver estável, a taxa de amostragem é reduzida. Quando ocorre uma variação de desempenho, a taxa de amostragem é elevada momentaneamente a fim de confirmar que se trata de uma mudança de tendência. O gráfico de controle resultante também serve como um resumo do desempenho da rede, simplificando a verificação da conformidade de acordos de SLA pré-estabelecidos.

Para testar o comportamento do algoritmo, de acordo com os objetivos desse trabalho, foram definidos alguns cenários de testes, realizados em laboratório, monitorando-se o desempenho de um tráfego VoIP trafegando em uma rede de desempenho variável devido a condições induzidas de congestionamento. Estes cenários foram construídos de forma a avaliar o comportamento do algoritmo em diversas situações, comparando-se a capacidade do algoritmo em capturar o comportamento real da rede. Dois parâmetros foram utilizados para avaliar o algoritmo proposto em cada um dos cenários: aderência e eficácia. A aderência foi definida como a capacidade do algoritmo de medição em capturar o verdadeiro comportamento da rede utilizando apenas uma amostragem parcial dos pacotes trafegados pela rede. A eficácia foi definida como sendo a capacidade do algoritmo de economizar amostras, isto é, de realizar o acompanhamento da rede com a menor quantidade possível de amostras. Deve-se, contudo enfatizar que esses parâmetros são conflitantes, e podem ser ajustados por parâmetros de operação do algoritmo. Nesse trabalho a aderência foi escolhida como prioritária em relação à eficácia.

O restante desse artigo está organizado da seguinte maneira. A seção 2 apresenta um resumo dos métodos de medição em redes IP. A sessão 3 apresenta a métrica MDI (Media Delivery Índex), escolhida como métrica de desempenho neste trabalho para acompanhamento do desempenho da rede no transporte de tráfego VoIP. A sessão 4 apresenta um embasamento sobre CEP, necessária a compreensão desse trabalho. A seção 5 apresenta o algoritmo proposto. A seção 6 apresenta os resultados dos testes realizados em laboratório. Finalmente, a conclusão apresenta um resumo dos resultados obtidos e aponta para desenvolvimentos futuros.

2. Medições em Redes IP

A monitoração de tráfego pode ser feita de forma passiva ou forma ativa. Na primeira, os pacotes capturados fazem parte do tráfego existente, não havendo necessidade de

injetar tráfego de teste na rede. Entretanto, deve-se ter como premissa que tal tipo de monitoração pode ser somente aplicado onde o tráfego de interesse já está presente na rede, o que é o caso da maioria das aplicações, onde se deseja validar o SLA ou efetuar engenharia de tráfego [ZSEBY, 2002 e 2004]. Já na monitoração ativa os pacotes são injetados com o objetivo de medir certas características da rede. Medições ativas são experimentos controlados que podem ser executados em qualquer momento e em qualquer padrão de tráfego de interesse, para um objetivo específico de monitoração. Entretanto, algumas desvantagens, como a inclusão de tráfego de testes, gerando tráfego adicional e questões de segurança, devem ser levadas em conta durante a escolha do método de monitoração (ver, por exemplo, [SHALUNOV, 2004]). Para avaliações de SLA, deve-se ter cuidado com a inserção de pacotes na rede, pois o mesmo deve ser tratado da mesma forma de um tráfego existente, para que as medições tenham precisão [ZSEBY, ZANDER & CARLE, 2001].

O *perfSONAR (Performance Service Oriented Network Monitoring Architecture),* desenvolvida pelo *Joint Research Activity 1 (JRA1)* é um modelo composto pelas duas formas de monitoração [HANEMANN *et al.*,2006]. Nele foram feitas três composições para análise de tráfego cujo caminho envolve redes distintas: agregação de tráfego em tempo, de dados em espaço e concatenação em espaço, para a qual foi apresentada uma análise de atraso (*one-way delay)* e a validação do procedimento proposto para obtenção de desempenho em caminhos fim a fim.

O PSAMP (*Packet Sampling)* é um conjunto de processos que define um método de monitoração que utiliza técnicas estatísticas de amostragem de dados, sua motivação vem da necessidade de um modelo de suporte a monitoração para fins de gerenciamento de rede, que represente precisamente e sem erros, as informações pertinentes ao estado dela no dado momento em que os pacotes foram capturados [CLAISE, 2006]. Este modelo define várias etapas do processo de amostragem, que inclui estratégias de seleção (filtragem ou amostragem), contagem e exportação dos dados coletados [DUFFIELD, 2007]. As operações nos métodos de seleção são divididas em dois subgrupos: seleção independente do conteúdo ou determinística *(content-independent sampling)* e seleção dependente do conteúdo (*content-dependent sampling*).

[ZSEBY *et al.*, 2007] apresentam uma discussão das técnicas de amostragem usadas pelo PSAMP. Este trabalho utiliza a técnicas de seleção baseada em contagem sistemática, conforme definido pelo PSAMP.

3. MDI - Media Delivery Index

O MDI (Media Delivery Index) é uma nova métrica definida pelo IETF que provê uma medida indicativa da necessidade da quantidade de *buffer* no ponto de destino para atenuar o efeito do *jitter*, assim como indicar possível perda de pacotes [WELCH, J. & CLARCK, 2006]. Permite identificar rapidamente, através da monitoração constante dos dados de aplicativos de tempo real em diversos pontos da rede e em situações de cargas distintas, dispositivos ou pontos que introduzem *jitter* significativo ou perda de pacotes, pela qual é possível realizar um novo planejamento de capacidade [INEOQUEST, 2005a e 2005b]. Como o tráfego de VoIP tem requisitos de qualidade de serviço semelhantes ao tráfego de vídeo, a metodologia para cálculo de MDI pode ser aplicada de forma igual. Assim, o MDI provê a informação necessária para detectar todos os

impedimentos causados pela rede para aplicações como VoIP e vídeo, que utilizam o protocolo UDP para transporte dos dados [AGILENT, 2008]. O MDI define duas métricas, denominadas DF (Delay Factor) e MLR (Media Loss Rate).

Para detalhar o cálculo de DF, considere o buffer virtual (VB) usado para receber pacotes de um fluxo de pacotes. Quando o pacote P(i) chega durante um intervalo de cálculo, dois valores de VB devem ser computados: VB(pré) e VB(pós), sendo que ambos os valores indicam a diferença de bytes recebidos e escoados. O valor do buffer virtual VB(i,pre) equivale ao tamanho buffer virtual antes da chegada de P(i) e o valor de buffer virtual VB(i,pos) equivale ao tamanho buffer virtual após chegada de P(i) [WELCH, J. & CLARCK, 2006].

$VB(i, pre) = \sum(Sj) - MR * Ti$ $onde\ j=1 .... i-1$ $VB(i,pos) = \sum(Sj) + Si$	Sj = *tamanho do payload do pacote j* Ti = *tempo relativo que o pacote i chega no intervalo* MR = *taxa nominal de transferência dos dados*

A condição inicial $VB(pre) = 0$ é usada no início de cada intervalo de medida. Após obtenção dos valores de VB(pré) e VB(pós) para um cada um dos pacotes recebidos, deve ser calculado o valor de VB(Max) e VB(min), que indicam o máximo e mínimo valor de buffer virtual necessário. O valor de DF para o para o intervalo de medida é calculado da seguinte forma:

$$DF = [VB(máximo) - VB(mínimo)] / MR$$

O valor geral aceitável de DF pode ser considerado entre 9 e 50ms. O outro componente denominado MLR *(Media Loss Rate)* consiste na contagem de pacotes perdidos ou fluxo de pacotes fora de ordem em determinado segundo. Estes são importantes, pois em muitos casos, não há reordenação de pacotes nos dispositivos de média dos clientes [AGILENT, 2008].

O MLR é computado através da subtração do número de pacotes recebidos, durante o intervalo de medida definido, e o número de pacotes esperados dividido pelo tamanho di intervalo definido, tendo valor máximo aceitável próximo de zero, pois qualquer perda de pacotes poderá afetar a qualidade de voz ou vídeo.

Neste artigo, apenas a métrica DF do MDI foi utilizada, por esta ser mais sensível aos problemas de congestionamento da rede, e mais fácil de induzir alterações através dos experimentos em laboratório.

4. CEP - Controle Estatístico de Processos

As técnicas de CEP (Controle Estatístico de Processo) são baseadas na construção de gráficos de controle, conforme a Figura 1. Um dos principais propósitos dos gráficos de controle é detectar ocorrências de mudança no processo, para que uma investigação da causa e uma ação corretiva possa ser tomada da forma mais rápida possível.

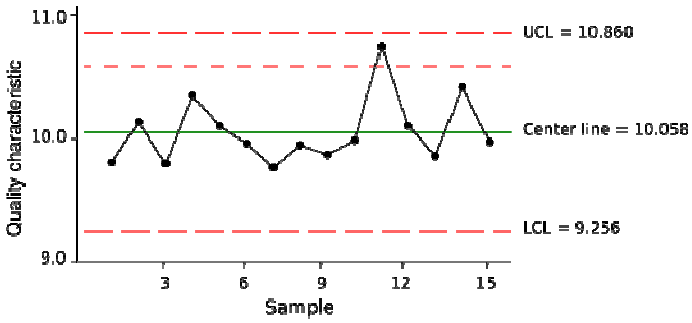


Figura 1. Exemplo de gráfico de controle X-barra

Quando um ponto de controle do gráfico fica fora dos limites de controle, considera-se que o processo está fora do controle estatístico. É desejável que um processo esteja em controle estatístico, para que seu comportamento seja previsível. Os gráficos de controle podem ser divididos em variáveis (usados para acompanhar grandezas contínuas) e de atributos (usados para acompanhar grandezas discretas, como falhas ou defeitos). Quando uma característica de qualidade é variável é uma prática comum controlar além do valor da média a variabilidade através de um gráfico de controle para médias, denominado gráfico do tipo X-barra [MONTGOMERY, 2005]. O gráfico de X-barra é composto por um processo com média μ e o desvio padrão σ. Supõe-se que o processo seja monitorado através de amostras periódicas, chamadas subgrupos de tamanho n e que a média computada para cada amostra seja X.

É usualmente assumido que a característica medida de um processo seja normalmente distribuída [NIST, 2009]. Nessas condições, a hipótese que guia a utilização dos gráficos de controle é que, em um processo estável, a grande maioria das mostras feitas de uma característica de qualidade deve estar contida no intervalo $\mu \pm 3\sigma$. Dessa forma, os limites de controle superior e inferior são usualmente escolhidos como: $UCL = \mu + 3\sigma$ *e* $LCL = \mu - 3\sigma$. Contudo, podem-se utilizar também linhas auxiliares $\mu \pm 2\sigma$ para melhorar o acompanhamento do processo e antecipar tendências. Para verificação do controle estatístico do processo observa-se como os pontos medidos se distribuem entre a média e o 2σ (comportamento controlado), entre o 2σ e o 3σ (possível mudança de tendência) e acima de 3σ (processo fora de controle ou em nova situação) [BARBETTA, 2004].

5. Proposta de Algoritmo de Amostragem Dinâmica baseado em CEP

O algoritmo proposto utiliza taxas de amostragem dinâmicas, que são ajustadas em intervalos regulares de tempo denominadas "janelas". No uso tradicional do CEP, as linhas de controle são fixas, pois elas refletem as condições da operação normal, supostamente conhecidas, do processo observado. Na estratégia desenvolvida nesse trabalho, as próprias linhas de controle do gráfico de CEP são recalculadas, periodicamente, de maneira refletir as alterações no comportamento da rede. O objetivo dessa operação é fazer com que as linhas do gráfico de CEP funcionem como um resumo do desempenho da rede, permitindo identificar facilmente os períodos no qual o desempenho da rede foi significativamente degradado, e também o momento em que a

rede retornou as suas condições de operação normal. Essa informação é relevante para o acompanhamento de contratos de SLA.

A estratégia considerada pode ser resumida como segue. Inicialmente, defini-se um comportamento padrão para rede (denominado baseline). Enquanto a rede permanecer nesse comportamento padrão, a taxa de amostragem é reduzida. A redução da taxa de amostragem é desejável, mas introduz erros de medição que podem ser falsamente interpretadas como alterações no comportamento do processo. Por isso, quando ocorrem alterações no comportamento da rede, a taxa de amostragem é aumentada temporariamente, até que o novo comportamento se estabilize, quando a taxa de amostragem é novamente reduzida.

Assumindo-se uma distribuição normal, as condições de controle foram definidas da seguinte forma:

a) Porcentagem de pontos esperadas entre $\mu \pm 2\sigma$: 95,44%

b) Porcentagem de pontos esperadas entre $\mu \pm 3\sigma$: 99,73%

c) Porcentagem de pontos de controle entre $\mu + 2\sigma$ e $\mu + 3\sigma$: 2,14%

d) Porcentagem de pontos de controle entre $\mu - 2\sigma$ e $\mu - 3\sigma$: 2,14%

Os testes “c)” e “d)” são necessários para determinar redução na variabilidade do processo. A algoritmo que implementa essa estratégia de amostragem pode ser resumido como segue:

Passo 1. (Re)definir o comportamento padrão da rede (baseline), determinando-se as linhas μ, $\mu + 2\sigma$ e $\mu \pm 3\sigma$ do gráfico de controle. Tal definição pode ser pré-definida para a na rede (comportamento desejado imposto pelas condições do SLA) ou calculada observando os pacotes durante uma "janela" sem amostragem (100% dos pacotes transmitidos são observados), em um período em que a rede esteja com desempenho considerado normal.

Passo 2. Monitorar o comportamento da rede durante NJ "janelas" utilizando a taxa de amostragem "alta". Caso o processo estiver controlado, ir para o Passo 3. Caso o processo esteja fora de controle, redefinir o comportamento padrão da rede (baseline), determinando-se as linhas μ, $\mu \pm 2\sigma$ e $\mu \pm 3\sigma$ do gráfico de controle, utilizando os dados coletados na última janela e voltar ao início do Passo 2.

Passo 3. Monitorar o comportamento da rede durante uma janela utilizando uma taxa de amostragem "baixa". Caso o processo esteja controlado, continuar no Passo 3, na próxima janela. Caso o processo esteja fora de controle, voltar ao Passo 2.

A Tabela 1 resume os parâmetros que controlam o comportamento do algoritmo. O modelo de amostragem utilizado é de amostragem sistemática por contagem, ou seja, a cada N valores amostrados na janela, um é escolhido randomicamente, sem repetição e, assim, sucessivamente, até atingir a taxa de amostragem escolhida para a janela [ZSEBY et al., 2007].

Segue uma breve discussão sobre o efeito esperado de cada um dos parâmetros controláveis do algoritmo. *Janelas* muito grandes farão com que o sistema “perca” transições rápidas de comportamento da rede. *Janelas* muito pequenas, por outro lado, irão introduzir oscilações indesejáveis com inúmeros recálculos das linhas de CEP. As

taxas de amostragem representam economias de processamento e armazenamento no sistema de medição, sendo que por esse critério valores baixos são desejáveis. Contudo, valores excessivamente baixos irão introduzir falsas interpretações de variação no processo, implicando em recálculos constantes do baseline e manutenção permanente da taxa de amostragem alta. A *tolerância* é necessária, uma vez que não se pode esperar que um processo amostral reproduza com infinita precisão a distribuição normal hipotética. O valor da *tolerância* não pode ser muito alto, sob o risco de mascarar mudanças de comportamento no processo. O número *NJ* é necessário para evitar que o sistema entre em oscilação, quando a amostragem baixa indicar o processo fora de controle. Isso irá ocorrer especialmente se a tolerância for muito pequena.

Tabela 1. Parâmetros controláveis do algoritmo

Parâmetro	Descrição
janela	Tempo com uma taxa de amostragem fixa (em segundos).
amostragemAlta	Porcentagem de pacotes amostrados (seleção randômica de um pacote a cada N pacotes) quando o estado de controle do processo for incerto.
amostragemBaixa	Porcentagem de pacotes amostrados (seleção randômica de um pacote a cada N pacotes) quando o processo estiver estável (controlado).
tolerância	Diferença máxima aceitável entre as porcentagens de pontos observados e as previstas pela distribuição entre as faixas de $\mu \pm 2\sigma$ e $\mu \pm 3\sigma$.
NJ	Número de janelas em amostragem alta que devem ser monitoradas antes de comutar a amostragem para baixa.

6. Estudo de Caso

O algoritmo proposto foi avaliado em quatro cenários distintos, denominados Normal, Transitório, Recorrente e Mudança Permanente. Em todos os cenários um fluxo de VoIP foi transportado em uma rede sujeita a congestionamento. Os cenários foram criados em uma rede de laboratório, onde diferentes níveis de congestionamento foram injetados na rede, a fim de causar impacto no desempenho da entrega de pacotes. A intensidade, duração e periodicidade dos eventos de congestionamento foram variadas em cada cenário, a fim de submeter o algoritmo proposto a uma ampla variedade de situações de operação. A métrica observada em todos os cenários foi o DF do MDI. Esta métrica foi escolhida por ser considerada a métrica mais completa para avaliação do desempenho de tráfego em tempo real, e também por ser a mais sensível a erros de medição, o que permite qualificar melhor o desempenho do algoritmo proposto.

Para realizar a validação do algoritmo, para cada uma das janelas de tráfego definidas foi calculada a aderência do algoritmo, que é uma medida da capacidade do

algoritmo em detectar as transições produzidas nos cenários. O cálculo da aderência para cada uma das janelas é feito da seguinte forma:

a) São verificados os pontos dentro e fora dos limites de $\mu \pm 3\sigma$

b) É calculada a aderência desta janela, ou seja, o percentual de pontos que ficou dentro dos limites $\mu \pm 3\sigma$

c) Ao final do processamento de todas as janelas é calculada a aderência total, que é a média da aderência de cada uma das janelas.

A ferramenta utilizada para cálculo das métricas e simulações neste trabalho é o *R*, que é linguagem e um ambiente de desenvolvimento integrado, para cálculos estatísticos e gráficos [R-PROJECT, 2010].

Para captura dos dados em rede, foi utilizada a ferramenta *Wireshark*, que é software livre e possibilita a captura, análise e realização de diagnósticos do tráfego de rede. O *Wireshark* provê funcionalidades muito similares ao *tcpdump* com uma interface gráfica e muito mais informações sobre opções de visualização e possibilidade de filtro de captura. A taxa nominal considerada para cálculo de DF, foi a de transmissão obtida através de detalhes da coleta, na ferramenta *Wireshark*.

A Figura 2 ilustra a topologia da rede usada para avaliação do algoritmo. Neste cenário um departamento remoto é conectado até uma central através de um enlace MPLS, com 512Kbps de capacidade, fornecido por uma operadora de telecomunicações. Os aparelhos telefônicos IP são conectados através de um switch Cisco 3560. O monitoramento dos dados foi feito espelhando-se a porta do switch ao qual o aparelho IP está conectado. A função de PABX IP é desempenhada pelo equipamento Cisco Call Manager, conectado na central.

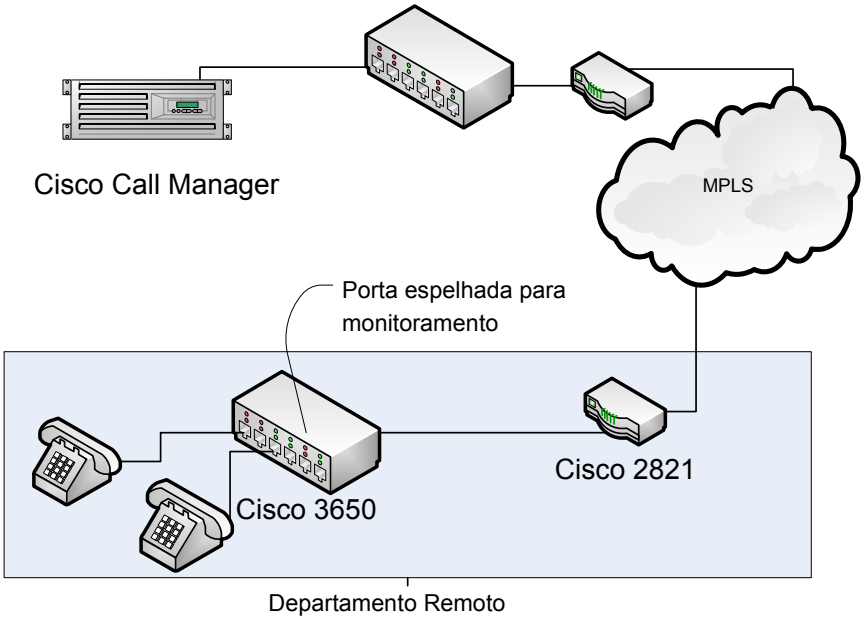


Figura 2. Topologia da rede onde foram capturados os dados.

O *codec* utilizado para transmissão de dados de voz nas chamadas executadas para captura foi o G.729, um algoritmo de compressão de voz que tem como requisito a

baixa utilização de banda, operando originalmente em taxas de 8 *kbits/s*, podendo haver extensões que operam em até 11.9 *kbits/s*.

Para simular as condições de congestionamento da rede foi utilizada a ferramenta para geração de tráfego *iperf* e desabilitando as políticas de QoS para a classe de voz no roteador Cisco 2821. O objetivo do tráfego gerado e da retirada das políticas de QoS é fazer com que os tempos de entrega dos pacotes de voz aumente e que conseqüentemente os valores do *delay factor* também variem. Com esta variação é possível testar o comportamento do algoritmo de amostragem dinâmica.

A ferramenta *ClearSight Network Analyzer* da empresa *ClearSight*, é uma aplicação para monitoração e fácil identificação de problemas em rede, com suporte a IPTV e um analisador para qualidade de métricas para Voz sobre IP. Como a ferramenta também mostra os valores da métrica de DF do MDI, foram utilizados os mesmos arquivos de captura para comparativos de valores obtidos com essa ferramenta e aqueles calculados pelo algoritmo proposto.

Tabela 2. Valores de DF para arquivo com 2682 pacotes RTP

Taxas Nominais	DF Médio	DF Máximo	DF Mínimo
Taxa Nominal 10,1 kips (Wireshark)	434, 7805	460, 9108	408, 6023
(% comparado ao DF calculado pelo ClearSight)	76,14%	74,10%	74,43%
Taxa Nominal 10, 894 kips (ClearSight)	466, 39784	492, 6617	437, 6339
(% comparado ao DF calculado pelo ClearSight)	81,68%	79,21%	79,71%
Valores Clearsight	571	622	549

A Tabela 2 mostra uma comparação entre os dados obtidos em uma coleta de 2682 pacotes. Como pode ser observado, os valores de DF médio, calculados pelo algoritmo desenvolvidos na ferramenta *R* são, em média, 80% do valor calculado pela ferramenta *ClearSight Analyzer*. Esta diferença é atribuída ao uso do *header* do protocolo RTP considerado como *payload* e também à diferença entre a taxa nominal calculada pelas ferramentas *Wireshark* e *ClearSight Analyzer*.

De forma empírica, para os cenários de testes apresentados a seguir, os seguintes valores foram considerados apropriados para as características da rede e da grandeza medida: *janela* = 60 segundos, *amostragemAlta* = 60%, *amostragemBaixa*=30%, *tolerância*=10%, *NJ*=3. Esses valores escolhidos induzem a uma economia modesta na taxa de amostragem, mas a uma aderência bastante elevada. Tais características foram consideradas apropriadas para o monitoramento dos fluxos VoIP através da métrica DF, muito sensível as oscilações de desempenho da rede. O monitoramento de desempenho de outros tipos de tráfego, como dados com requisitos de desempenho elásticos, poderá usar taxas de amostragem bastante inferiores.

A métrica DF foi calculada em intervalos de 1 segundo. Isto significa que existem 60 medidas disponíveis por janela. Quando a amostragem alta é utilizada, são feitas 36 medidas, e quando a amostragem é baixa são feitas 18 medidas.

6.1. Cenário Normal

Neste cenário foram capturados pacotes de uma chamada de voz com nível de qualidade dentro do esperado, sem variação de tráfego ou mudança nos mecanismos de controle da qualidade do serviço. A figura 3 mostra os resultados desse experimento.

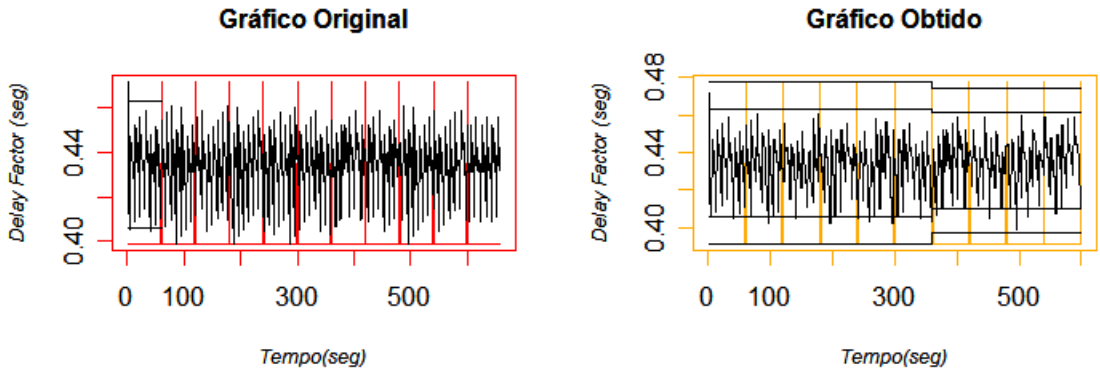


Figura 3. Gráfico Original e Gráfico Obtido através do algoritmo de amostragem dinâmica para cenário normal

O Gráfico Original mostra os valores de DF calculados, já o Gráfico Obtido mostra como as linhas de controle foram traçadas para acompanhar as variações do processo. O eixo *x* representa o tempo da coleta em segundos, cada uma das linhas verticais que cortam este eixo, representa a janela de tempo definida de 60 segundos, para cada janela de tempo o algoritmo executa a amostragem dinâmica e realiza as validações do *baseline*. O eixo *y* representa o valor da métrica de *delay factor* (DF), calculada para cada segundo, conforme algoritmo para cálculo descrito anteriormente.

Para este cenário, conforme pode ser verificado na Figura 6, no gráfico obtido não houve variação da métrica nos primeiros 360 segundos da coleta total. Após este intervalo, uma pequena variação no valor de UCL e LCL ocorreu, pois o algoritmo considerou as pequenas oscilações da rede como uma variação de comportamento, e efetuou o recálculo do *baseline.*

Tabela 3. Detalhamento dos resultados obtidos para o Cenário Normal

Janela	Tempo Inicial	Tempo Final	Taxa de Amostragem	Qtde Amostras	Amostras fora de $\mu \pm 3\sigma$	Amostras entre 2σ e 3σ	Amostras dentro de $\mu \pm 2\sigma$
1	0	60	Calculando Baseline				
2	61	120	60%	36	0	3	33
3	121	180	60%	36	0	2	34
4	181	240	60%	36	0	3	33
5	241	300	30%	18	0	1	18
6	241	300	30%	18	0	2	16
7	301	360	30%	18	0	2	16
8	361	420	30%	18	0	4	15
9	421	480	60%	36	0	4	33
	421	480	Recalculo do baseline				
10	481	540	60%	36	0	2	34
11	541	600	60%	36	0	3	33

A Tabela 3 mostra os resultados relacionados a esse cenário. A quantidade de pontos do gráfico original no intervalo μ ± 3σ é de 100%, considerando que μ e σ são definidos com os dados da primeira janela. Isto significa que os dados sofreram pequena variação nas demais janelas do experimento, o que caracteriza um cenário bem comportado. A aderência calculada para o gráfico obtido através do algoritmo de amostragem foi de 90%. A taxa média de amostragem foi de 48%, uma vez que 6 janelas usaram amostragem alta e 4 janelas utilizaram amostragem baixa.

6.2 Cenário Transitório

Neste cenário foram simuladas perdas de qualidade devido ao aumento de tráfego na rede e falta de políticas de QoS adequadas para garantir a qualidade do serviço de voz.

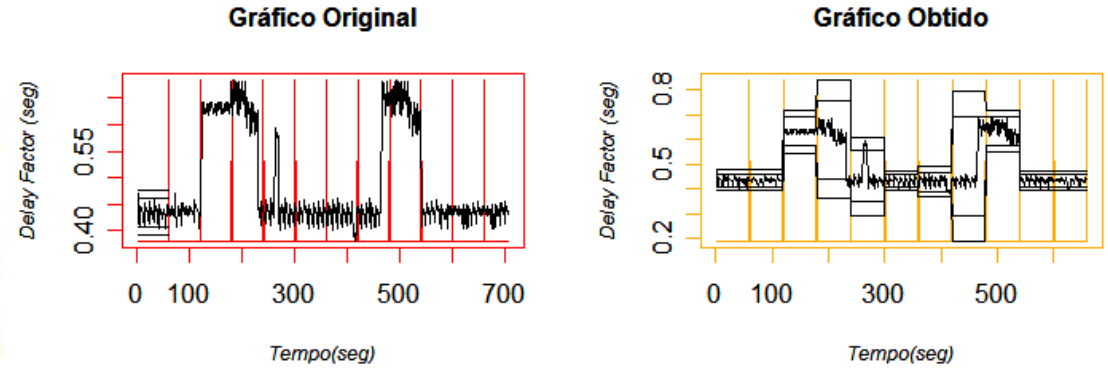


Figura 4. Gráfico original e gráfico obtido através do algoritmo de amostragem dinâmica cenário transitório

Na Figura 4 pode ser observado o resultado do algoritmo para o cenário transitório. O experimento teve duração total de 720 segundos, dividido em 12 janelas de 60 segundos. Neste cenário, ocorreram vários cálculos de novo valor de *baseline*, tendo em vista a variação da métrica DF. Isso pode ser percebido pelas variações nas linhas de UCL e LCL no gráfico obtido. A quantidade de pontos do gráfico original no intervalo μ ± 3σ é de 71%, o que mostra grande variabilidade do tráfego em relação ao *baseline* calculado na primeira janela. Neste cenário a aderência calculada para o gráfico obtido através do algoritmo de amostragem dinâmica é de 98.3%. A taxa de amostragem foi de 60%, uma vez que durante o período de testes o processo não permaneceu em controle por tempo suficiente a fim de migrar para uma taxa de amostragem mais baixa.

Observa-se que o algoritmo foi capaz de detectar tanto as variações de comportamento, quanto o retorno as condições normais de operação, o que permitiu atingir um nível muito alto de aderência.

6.3. Cenário Recorrente

Neste cenário foram simuladas perdas de qualidade devido ao aumento de tráfego na rede de forma a obter um cenário recorrente, onde alterações no valor da métrica ocorrem de forma semelhante em determinados períodos de tempo.

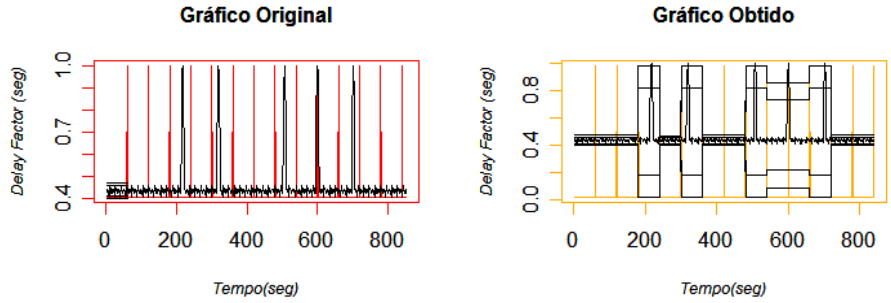


Figura 5. Gráfico original e gráfico obtido através do algoritmo de amostragem dinâmica em Cenário Recorrente

Neste cenário, o objetivo é testar a capacidade do algoritmo de reconhecer mudanças recorrentes de comportamento e voltar ao valor de *baseline* correto após as alterações de perfil. Nesse caso, 98% dos pontos do gráfico original ficaram no interior do limite de $\mu \pm 3\sigma$. A aderência do gráfico obtido foi de 94%. A taxa média de amostragem foi de 60%, pois o sistema não pode entrar em processo de amostragem baixa.

6.4. Mudança Permanente de Comportamento

Neste cenário, optou-se por gerar uma carga fora do comportamento normal do *link* em questão, de forma que o valor do DF sofresse uma degradação em um período grande tempo, sugerindo assim, uma mudança permanente de perfil. A figura 6 ilustra os resultados obtidos nesse cenário.

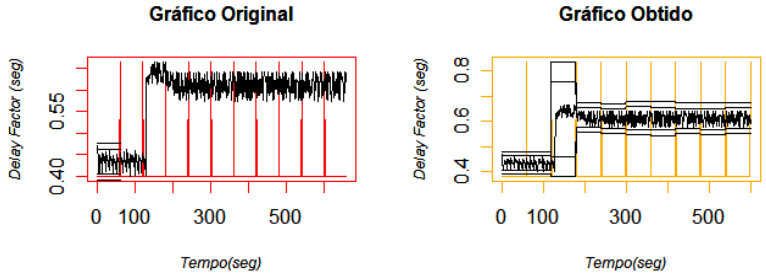


Figura 6. Gráfico original e gráfico obtido através do algoritmo de amostragem dinâmica para Cenário com mudança permanente de comportamento

No gráfico original, localizado à esquerda da Figura 6, pode ser verificado que o comportamento do tráfego a partir da janela 3 é alterado significativamente. As linhas de UCL e LCL da primeira janela após a transição são amplas, pois elas capturaram a brusca variação no processo. Após a primeira grande transição, os valores de *baseline* foram re-calculados várias vezes, em alguns casos devido ao fato da própria mudança de comportamento da rede e em outros, devido a erros introduzidos pelo processo de amostragem. Isso impediu que o algoritmo voltasse a uma taxa de amostragem baixa, indicando que a tolerância de 10% adotada para esses testes foi muito pequena. Nesse caso, a quantidade de pontos do gráfico original no intervalo $\mu \pm 3\sigma$ foi 90%. A aderência do gráfico obtido foi de 95%. A taxa de amostragem média foi de 75,5%, uma vez que as oscilações após a transição brusca de comportamento impediram que o algoritmo entrasse numa fase de amostragem baixa.

7. Conclusão

O estudo de técnicas de amostragem de dados é bastante relevante, pois oferece uma solução para minimizar a quantidade de dados analisados e simplificar o processo de análise de contratos de prestação de serviços de comunicação regidos por acordos de SLA. Este estudo avaliou uma nova estratégia de amostragem, baseada na utilização de gráficos de controle do tipo CEP, para controlar a taxa de amostragem e resumir os principais eventos de variação de comportamento da rede. Nesse estudo, constatou-se que a métrica DF, do MDI, oferece uma nova abordagem para o monitoramento do desempenho do transporte de tráfego em tempo real. Tal métrica ainda é relativamente nova, mas está sendo introduzida gradativamente na indústria, pela sua incorporação de ferramentas comerciais de monitoramento. A análise dos resultados em quatro cenários distintos demonstrou que a abordagem pode ser parametrizada para obter excelentes resultados em relação a sua capacidade de capturar as mínimas variações de desempenho da rede. Quanto mais comportado for o desempenho da rede, menos amostras são utilizadas. Os resultados, por outro lado, mostraram também que os limites de controle tradicionais baseados nas linhas de $\mu \pm 2\sigma$ e $\mu \pm 3\sigma$ podem ser excessivamente rígidos dada a grande variabilidade inerente ao desempenho da rede, como se pode observar, especialmente, no quarto cenário, onde as oscilações naturais da rede impediram uma estabilização em taxas de amostragem baixas.

A gama de possibilidades para construção de técnicas de monitoramento baseada em CEP é muito grande, sendo que esse artigo abordou apenas alguns aspectos possíveis. Uma abordagem promissora é o uso mais faixas de freqüências de amostragem possíveis, que permitam que o algoritmo progrida continuamente para taxas de amostragem menores, na medida em que o desempenho da rede se mantém estável. Outras melhorias possíveis são o uso de tolerâncias dinâmicas, que cresçam quando a rede esteja com desempenho muito superior ao mínimo desejado e se reduzam automaticamente na medida em que ela se aproxime dos limites exigidos.

Referencias

AGILENT Techonologies, White Paper (2008). IPTV QoE: Understanding and interpreting MDI values. France, September 29, 2008.

BARBETTA, Pedro Alberto (2004). Estatística para Cursos de Engenharia e Informática. São Paulo: Atlas, 2004.

CISCO Systems (2006). Understanding Delay in Packet Voice Networks. Disponível em http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml. Acesso em 02/02/2006.

CLAISE, B. (Ed.) (2006). Packet Sampling (PSAMP) Protocol Specifications. Currently Internet (work in progress) Draft draft-ietf-psamp-protocol-07.txt., 2006.

DUFFIELD, Nick (Ed.) (2007) .A Framework for Packet Selection and Reporting. Currently Internet Draft (work in progress) draft-ietf-psamp-framework-11, 2007.

HANEMANN et al. (2006). A Study on Network Performance Metrics and their Composition: (1) German Research Network, (2) Greek Research & Technology Network S.A, (3) DANTE, (4) Dep. of Computer and Information Sciences, University of Delaware. USA: March.

INEOQUEST Technologies, Inc. (2005a). Media Delivery Index – Application Note 5. USA: May 20, 2005.

INEOQUEST Technologies, Inc.(2005b). MDI/QoE para IPTV e VOIP. USA: July 2, 2005b.

MONTGOMERY, D. C. (2005). Introduction to Statistical Quality Control. New York: Wiley.

NIST – National Institute of Standards and Technology (2009). Process or Product Monitoring and Controle. Disponível em http://www.itl.nist.gov/div898/handbook/pmc/pmc.htm. Acesso em 10/01/2009.

SHALUNOV et al (2004)., S. RFC 4656 - One-way Active Measurement Protocol (OWAMP). Draft-ietf-ippm-owdp-11.txt. Request for comments, 2004.

WELCH, J. & CLARCK, J. (2006). RFC 4445 - A Proposed Media Delivery Index (MDI).

ZSEBY, Tanja (2002). Deployment of Sampling Methods for SLA Validation with Non-Intrusive Measurements. Proceedings of Passive and Active MeasurementWorkshop (PAM 2002), Fort Collins, CO, USA, March 25-26, 2002.

ZSEBY, Tanja (2004). Comparison of Sampling Methods for Non-Intrusive SLA Validation. 2nd Workshop on End-to-End Monitoring Techniques and Services (E2EMON), October 3, 2004

ZSEBY, T.; ZANDER, S. & CARLE, G. (2001). Evaluation of Building Blocks for Passive One-way-delay Measurements. Proceedings of Passive and Active Measurement Workshop (PAM 2001). Amsterdam: The Netherlands, April 23-24.

ZSEBY et al. (2007). Tanja. Sampling and Filtering Techniques for IP Packet Selection. Currently Internet Draft (work in progress), draft-ietf-psamp-sample-tech-10.txt., 2007.

R-PROJECT (2010). The R Project for Statistical Computing. Disponível em http://www.r-project.org/. Acesso em 02/02/2010.

Desempenho do Roteamento Adaptativo-Alternativo em Redes Ópticas Dinâmicas

Paulo Ribeiro L. Júnior[1], **Michael Taynnan**[2], **Marcelo S. Alencar**[1]

[1]Departamento de Engenharia Elétrica (DEE)
Instituto de Estudos Avançados em Comunicações (Iecom)
Universidade Federal de Campina Grande (UFCG)
Campina Grande, PB – Brazil

[2]Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB)
Campus Campina Grande
Campina Grande, PB – Brazil

{paulo,malencar}@iecom.org.br, {michael.taob}@gmail.com

Abstract. *In this article, four routing approaches are compared from the point of view of blocking probability for two scenarios: first varying the offered load and then varying the number of wavelengths. The scenarios give a more complete picture of the performance of these routing approaches and may help decide which to use based on the routing topology and traffic characteristics. Among the possible benefits of choosing the correct routing approach to be used to highlight the expected decrease in the number of wavelengths to maintain a given number of blocks in the network.*

Resumo. *Nesse artigo, são comparadas quatro abordagens de roteamento do ponto de vista da probabilidade de bloqueio em dois cenários: variando-se a carga oferecida e variando o número de comprimentos de onda. Os cenários dão uma visão mais geral do desempenho dessas abordagens de roteamento que pode auxiliar na decisão de qual roteamento usar a partir das características de topologia e tráfego. Dentre os possíveis benefícios de uma escolha correta da abordagem de roteamento a ser utilizada se destaca a esperada diminuição no número de comprimentos de onda para se manter um dado número de bloqueios na rede.*

1. Introdução

A popularização da Internet e dos serviços a ela correlacionados propiciou aumento na de qualidade de serviço sobre a infra-estrutura das redes de comunicações, que está diretamente ligada a fatores como baixo atraso na transmissão, alta largura de banda disponível, alta disponibilidade e baixa taxa de interrupção de transmissão. As redes ópticas multiplexadas por divisão em comprimento de onda (WDM – *Wavelength Division Multiplexing*), devido, principalmente, às suas características físicas, tÊsm ganhado cada vez mais aceitação como meio de transporte promissor para o tráfego da Internet e de outras fontes que nescessitam dessas características de qualidade.

Os usuários dessas redes se comunicam por conexões ópticas fim-a-fim, denominadas caminhos ópticos (*lightpaths*), desde um nó origem até um nó destino em uma rede

óptica e que utilizam, na ausência de conversão de comprimento de onda, o mesmo comprimento de onda disponível em todos os enlaces que compõem o caminho entre esses nós.

O problema de estabelecer conexões em uma rede óptica envolve o uso de algoritmos de roteamento e alocação de comprimento de onda (RWA – *Routing and Wavelength Assignment*). Tipicamente, um caminho óptico era caracterizado pelo conjunto "rota mais comprimento de onda"; entretanto, em uma visão multi-cliente, caminhos ópticos na rede totalmente óptica podem possuir características diferentes dependendo da aplicação ou da rede cliente que os está solicitando [Fonseca 2005] [Ramaswami and Sivarajan 2002]. Sendo assim, além de uma rota e de um comprimento de onda, para sua melhor caracterização, é necessário que um caminho óptico possua também atributos de qualidade de serviço óptico associados à sua criação no contexto de rede totalmente óptica.

Nesse artigo são comparadas quatro abordagens de roteamento do ponto de vista da probabilidade de bloqueio. Essa comparação é feita variando o número de comprimentos de onda disponíveis em cada fibra óptica mas com um valor fixo de carga oferecida na rede e, depois, variando a carga oferecida na rede e mantendo fixo o número de comprimentos de onda.

Esses dois cenários dão uma visão mais completa do desempenho dessas abordagens de roteamento, gerando resultados que podem ajudar o operador e o projetista da rede a decidir que roteamento usar a partir das características de topologia e tráfego. Dentre os possíveis benefícios de uma escolha correta da abordagem de roteamento a ser utilizada se destaca a esperada diminuição no número de comprimentos de onda para se manter um dado número de bloqueios na rede. Tal característica se traduz em sistemas com menor custo de instalação e manutenção da rede. Por outro lado, se garante que a extensibilidade da rede projetada praticamente não será afetada, pois há a capacidade de se suportar um volume maior de tráfego.

O restante do artigo se apresenta da seguinte forma: na Seção 2 é apresentada uma visão geral das redes roteadas a comprimento de onda. Nessa seção também o problema do RWA é definido; na Seção 3 são apresentadas as abordagens clássicas para roteamento bem como uma visão do estado da arte referente ao tema discutido. Também é apresentado o algoritmo de roteamento adaptativo-alternativo; na Seção 4 são discutidos o ambiente de simulação e os resultados obtidos dos experimentos e, na Seção 5, são apresentadas as conclusões do trabalho.

2. Redes ópticas roteadas a comprimento de onda

Uma característica intrínseca e única das redes WDM roteadas a comprimento de onda é a estreita ligação entre o estabelecimento de rotas e a atribuição de comprimentos de onda. Como visto na Figura 1, o estabelecimento de um caminho óptico é implementado pela seleção de uma rota, composta de enlaces físicos, entre um nó origem e um nó destino e a alocação de um comprimento de onda específico para a conexão [Rouskas and Perros 2002]. O problema de prover caminhos ópticos a uma rede óptica é chamado de problema de Roteamento e Alocação de Comprimento de Onda ou simplesmente RWA [Zang et al. 2000] e é mais complexo do que o problema de roteamento em redes eletrônicas. A complexidade adicional surge pelo fato do estabelecimento de um caminho óptico estar sujeito a uma restrição, conhecida como restrição de

comprimento de onda, que estabelece que, na ausência de conversores de comprimento de onda, o caminho óptico precisa ocupar o mesmo comprimento de onda em todos os enlaces entre um nó origem e um nó destino da rede [Ramaswami and Sivarajan 2002]. Um exemplo dessa característica é ilustrada na Figura 1, na qual dois caminhos ópticos são estabelecidos contendo enlaces em comum nas suas rotas e, por conta disso, dois comprimentos de onda são necessários.

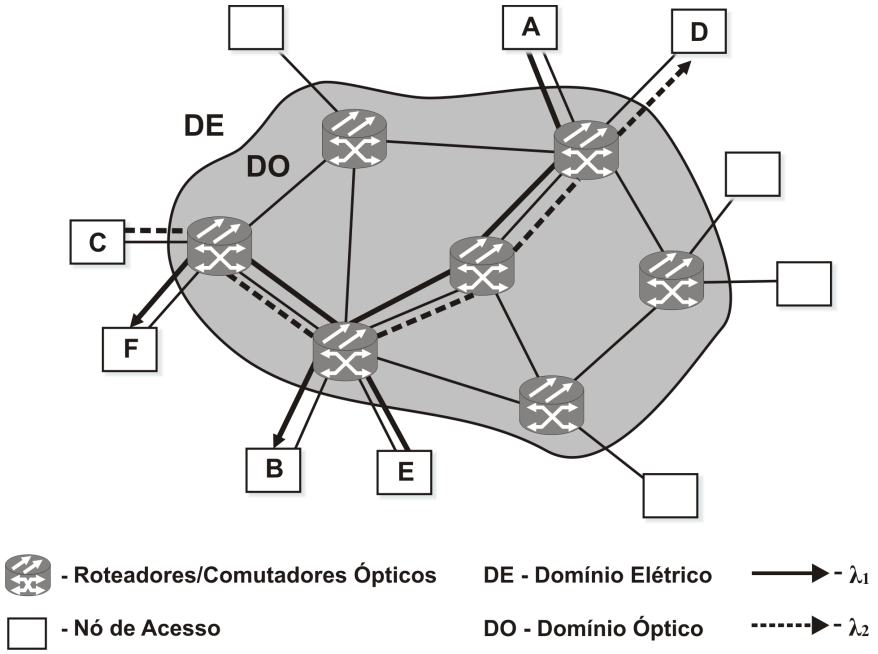


Figura 1. Representação de uma rede óptica transparente ilustrando a formação do domínio de transparência.

O problema pode ser apresentado da seguinte forma. Considere uma rede com K enlaces e W comprimentos de onda. O estado do i-ésimo enlace, $1 \leqslant i \leqslant K$, no instante de tempo t pode ser especificado pelo vetor coluna

$$\sigma_t^{(i)} = \begin{bmatrix} \sigma_t^{(i)}(1) \\ \sigma_t^{(i)}(2) \\ \vdots \\ \sigma_t^{(i)}(W) \end{bmatrix}, \tag{1}$$

em que, $\forall\ j$ tal que $1 \leqslant j \leqslant W$, $\sigma_t^{(i)}(j) = 1$ se o comprimento de onda j é usado por um caminho óptico no instante de tempo t, no enlace i e $\sigma_t^{(i)}(j) = 0$ se este comprimento de onda estiver disponível. Assim sendo, o estado da rede é descrito pela matriz

$$\sigma_t = \begin{bmatrix} \sigma_t^{(1)}(1) & \sigma_t^{(2)}(1) & \cdots & \sigma_t^{(K)}(1) \\ \sigma_t^{(1)}(2) & \sigma_t^{(2)}(2) & \cdots & \sigma_t^{(K)}(2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_t^{(1)}(W) & \sigma_t^{(2)}(W) & \cdots & \sigma_t^{(K)}(W) \end{bmatrix}. \tag{2}$$

Dada uma requisição para o estabelecimento de conexão óptica no instante de tempo t entre os nós origem e destino, a função do algoritmo de RWA é selecionar um caminho E, composto pelos enlaces $(e_1, e_2, \ldots, e_n)$, tal que $\sigma_t^{(e_l)}(j) = 0$ para todo $l = 1, 2, \ldots, n$. Tal consideração satisfaz a restrição de continuidade de comprimento de onda.

O problema do RWA pode se apresentar de diferentes formas. As diferentes variantes, entretanto, podem ser genericamente classificadas de duas formas: um RWA estático, chamado de estabelecimento estático de caminho óptico (SLE – *Static Ligthpath Establishment*), segundo o qual as requisições de tráfego são conhecidas *a priori* e as rotas e respectivas alocações de comprimentos de onda são estabelecidas antes da sinalização entre os nós componentes das rotas e um RWA dinâmico, chamado de estabelecimento dinâmico de caminho óptico (DLE – *Dynamic Ligthpath Establishment*), em que as requisições são estabelecidas no momento em que são solicitadas, de acordo com o estado atual da rede. Neste trabalho, considera-se apenas o estabelecimento dinâmico de caminhos ópticos.

Na operação dinâmica de uma rede, os nós submetem requisições ao plano de controle para o estabelecimento de caminhos ópticos de acordo com suas necessidades. Dependendo do estado da rede no momento da requisição, a disponibilidade de recursos pode ou não ser suficiente para o estabelecimento de um caminho óptico no par de nós origem e destino correspondente. O estado da rede consiste da informação acerca de todas as rotas físicas e comprimentos de onda utilizados pelos caminhos ópticos ativos e muda de maneira aleatória à medida que novos caminhos ópticos vão se tornando ativos ou inativos na rede. Dessa forma, cada vez que uma requisição é feita, um algoritmo precisa ser executado em tempo real para determinar se é possível estabelecer um caminho óptico para ela. Se a requisição para um caminho óptico não for aceita devido à falta de recursos, então ela será bloqueada.

Por serem executados em tempo real, algoritmos de RWA em ambiente de tráfego dinâmico precisam ser simples. Tendo em vista que tratar os problemas de roteamento e alocação de comprimento de onda de forma unificada é oneroso do ponto de vista computacional, uma abordagem típica para se desenvolver algoritmos eficientes é desacoplar o problema em dois sub-problemas: o problema do roteamento e o problema da alocação de comprimento de onda e tratá-los de forma independente [Zang et al. 2000]. Dessa forma, a maioria dos algoritmos de RWA dinâmicos para redes roteadas a comprimentos de onda consistem dos seguintes passos gerais:

- **1º Passo –** Escolher os enlaces físicos que comporão a rota para cada par de nós origem e destino, de acordo com alguma métrica estabelecida, podendo-se criar listas que enumerem as rotas desde a melhor até a pior;
- **2º Passo –** Ordenar os comprimentos de onda em uma lista de acordo com alguma métrica particular;
- **3º Passo –** Selecionar a melhor rota e o melhor comprimento de onda, de forma a tentar estabelecer o melhor caminho óptico possível.

A natureza específica de um algoritmo de RWA dinâmico é determinada pelo número de rotas candidatas e pela forma como elas são selecionadas a partir de uma lista de possibilidades, a ordem com que os comprimentos de onda são listados e a forma como

essas listas de rotas e comprimentos de onda são acessadas para se compor o caminho óptico requerido por uma rede cliente.

3. Roteamento

Se um algoritmo estático é usado no cálculo para a seleção das melhores rotas, estas são estabelecidas e ordenadas de forma descorrelacionada do estado da rede. Já se um algoritmo adaptativo é utilizado para tal fim, os rotas que comporão os possíveis caminhos ópticos bem como seu ordenamento podem variar dependendo do estado atual da rede. Um algoritmo estático é executado *off-line*, ou melhor, anteriormente ao processo de sinalização entre os nós para o estabelecimento do caminho e as rotas calculadas são ordenadas e armazenadas para um uso posterior, que leva à uma baixa latência na rede durante o estabelecimento do caminho óptico. Algoritmos adaptativos, por sua vez, são executados no momento em que é feita uma requisição por um caminho óptico e que os nós sinalizam para sua obtenção. Por esse motivo, é dito que eles são executados *on-line*.

3.1. Abordagens clássicas de roteamento

Tipicamente, de acordo com [Zang et al. 2000], três tipos de algoritmos de roteamento são utilizados em redes ópticas roteadas a comprimentos de onda:

- **Fixo –** Este método é a forma mais direta de seleção de rotas, pois configura uma rota permanente ou semi-permanente entre o par de nós origem e destino, selecionada por algum algoritmo que calcula o caminho de melhor custo entre dois pontos de um grafo (como o algoritmo de Dijkstra ou de Bellman-Ford, por exemplo). Esse tipo de algoritmo de roteamento tem como principal vantagem sua simplicidade. Entretanto, devido a uma grande sensibilidade à falhas na rede, se por algum motivo algum dos recursos reservados para o estabelecimento do caminho óptico sobre a rota pré-determinada estiver indisponível, a probabilidade de bloqueio de rede pode se tornar considerável, tanto para casos estáticos quanto para dinâmicos [Zang et al. 2000];
- **Alternativo –** Neste método considera-se a seleção de rotas alternativas à rota mais curta. Quando uma conexão é requisitada, o nó fonte tenta estabelecer uma conexão com o nó destino por meio de cada rota usando a tabela de roteamento, começando sempre pela rota de melhor custo. Caso a primeira não esteja disponível, a segunda rota de melhor custo é então utilizada e assim por diante até conseguir uma rota. Caso não seja encontrado um caminho disponível, a requisição é perdida. [Mukherjee 2006].
- **Adaptativo –** No roteamento adaptativo, a rota de um nó fonte a um nó destino é escolhida dinamicamente, dependendo do estado da rede, comumente relacionado com o número de caminhos ópticos ativos na rede. Nessa abordagem, o algoritmo faz atualizações na tabela de roteamento seguindo uma determinada métrica, geralmente especificada por uma ou mais funções custo. As funções possuem como argumento parâmetros da rede, que podem ser calculados ou mensurados e retornam um novo valor para o custo em um dado enlace, em consonância com seu estado atual. A tabela de roteamento é, então, atualizada com esses novos valores calculados, de forma que uma conexão estabelecida em um dado instante de tempo provavelmente não terá a mesma tabela de roteamento que a conexão estabelecida num instante de tempo anterior.

A literatura apresenta diversos trabalhos que tratam do problema do roteamento em redes ópticas WDM, mais especificamente de como estabelecer custos para os enlaces de redes ópticas, sejam elas estáticas ou dinâmicas, de forma a se conseguir, por exemplo, uma melhor distribuição dos recursos disponíveis na rede. Em especial, para as redes dinâmicas, a abordagem mais utilizada tem sido a consideração de custos adaptativos, seguindo funções predefinidas que tenham como argumentos os parâmetros da rede. [Karasan and Ayanoglu 1998] apresentam uma heurística de seleção dinâmica de rotas e de comprimentos de onda, baseada no caminho menos congestionado (LLR – *Least-Loaded Routing*). Uma abordagem denominada algoritmo de roteamento conjunto (JRA – *Joint Routing Algorithm*) é apresentada por [Wen et al. 2003] para roteamento adaptativo e comparada com outros algoritmos. [Mokhtar and Azizoglu 1998] adotam uma abordagem mais geral para o RWA adaptativo. O algoritmo proposto nesse trabalho considera todas as possíveis rotas entre um par de nós origem e destino e utiliza a informação do estado atual da rede para ponderar as rotas, de forma que a rota em melhores condições esteja no topo da lista das possíveis rotas. Uma abordagem similar é usada por [Dante 2005] com uma comparação entre três algoritmos clássicos de roteamento – o RIP (*Routing Information Protocol*), o OSPF (*Open Shortest Path Function*) e o IGRP (*Interior Gateway Routing Protocol*) – e o algoritmo WLC (*Weighted Link Capacity*) proposto. Já [Brunato et al. 2003] abordam o balanceamento de carga executado a partir de modificações na tabela de roteamento, na tentativa de se obter a melhor rota. Essa rota é analisada e buscada em um conjunto das rotas possíveis e seu uso configura, segundo os autores, a necessidade de modificação na tabela. [Fabry-Asztalos et al. 2000] realizam um estudo comparativo entre três métricas de roteamento adaptativo.

3.2. Roteamento adaptativo-alternativo

O principal objetivo desse trabalho é comparar o desempenho dos algoritmos mencionados anteriormente com uma abordagem mista, conhecida como algoritmo de roteamento adaptativo-alternativo.

No roteamento adaptativo-alternativo, assim como no adaptativo, as rotas são selecionadas de acordo com o estado atual da rede. A diferença entre os dois algoritmos consiste no fato de que no adaptativo alternativo são selecionadas todas as rotas disjuntas, ou seja, rotas que não disponham de enlaces em comum, entre um par de nós origem e destino. Em outras palavras, esse algoritmo é uma fusão do algoritmo alternativo e do algoritmo adaptativo.

Ao tentar selecionar uma rota entre um par de nós, o algoritmo adaptativo-alternativo seleciona todas as rotas disjuntas entre esse par de nós origem e destino, usando o estado atual da rede. Em seguida, essas rotas são ordenadas do menor para o maior custo. A rota escolhida será aquela que tiver comprimentos de onda disponíveis para serem alocados, de acordo com a heurística trabalhada. No caso desse trabalho, essa heurística é a *first-fit*. A estratégia do algoritmo *first-fit* é enumerar todos os comprimentos de onda e selecionar de ordem crescente aquele comprimento de onda disponível de menor índice da lista (primeiro disponível).

O algoritmo completo de RWA, usando roteamento adaptativo-alternativo e alocação de comprimento de onda *first-fit* é descrito no algoritmo 1.

Algoritmo 1 RWA com roteamento adaptativo-alternativo e *first-fit*

Entrada: topologia; nós origem (s) e destino (d)
Saída: rota e comprimento de onda selecionados entre os nós (s) e (d)

```
1: Algoritmo de Dijkstra seleciona todas as rotas disjuntas entre o par de nós (s) e (d) ;
2: As rotas selecionadas no passo anterior são alocadas no vetor R, ordenadas do menor
   para o maior custo;
3: enquanto um comprimento de onda λ não for selecionado ou a requisição não for
   bloqueada faça
4:    escolha da primeira rota em R;
5:    escolha do primeiro λ que esteja livre em todos os enlaces que compõe a rota
      selecionada;
6:    se houver λ disponível em todos os enlaces da rota então
7:       seleciona o λ e sai do laço;
8:    caso contrário
9:       retira a rota de R e continua no laço;
10:   fim
11: fim do laço 'enquanto'
12: se houve λ selecionado então
13:    atualiza os custos dos enlaces que compõe a rota selecionada;
14: caso contrário
15:    bloqueia o estabelecimento da conexão.
16: fim
```

4. Simulação e Resultados

Para avaliar o desempenho dos algoritmos estudados com relação à probabilidade de bloqueio foi feito uso de um simulador de redes ópticas dinâmicas desenvolvido pelos autores usando a linguagem de programação Python. A simulação de redes ópticas transparentes pode ser realizada levando em conta uma demanda de conexões estática, para uma matriz de tráfego estática definida antes da simulação e que não varia ao longo da execução, ou levando em consideração uma demanda de conexões dinâmica, que escolhe aleatoriamente os pares de endereços de origem e destino de uma conexão, o tempo de início da conexão e o período de duração da conexão. O simulador implementado considera um modelo de requisição de conexão dinâmico.

Para os experimentos são consideradas quatro topologias de redes distintas: um anel com nove nós (Figura 2 a)), que tem como característica a baixa quantidade de enlaces e nós com grau 2, uma topologia em malha regular, porém simples, com apenas cinco nós (Figura 2 b)), a topologia *Torus* em uma malha (*mesh-torus*) com 9 nós, tendo cada nó um grau 4 (Figura 2 c)) e uma topologia baseada na rede da *National Science Foundation*, conhecida como NSFNet, Figura 2 d).

Nas execuções da simulação, o critério de parada utilizado é o número de requisições de conexão. São contabilizadas as requisições de conexão e não apenas as conexões estabelecidas com sucesso. Um número significativo de requisições de conexão é executado de maneira que o efeito transitório inicial seja desprezível e o regime permanente de operação da rede predomine.

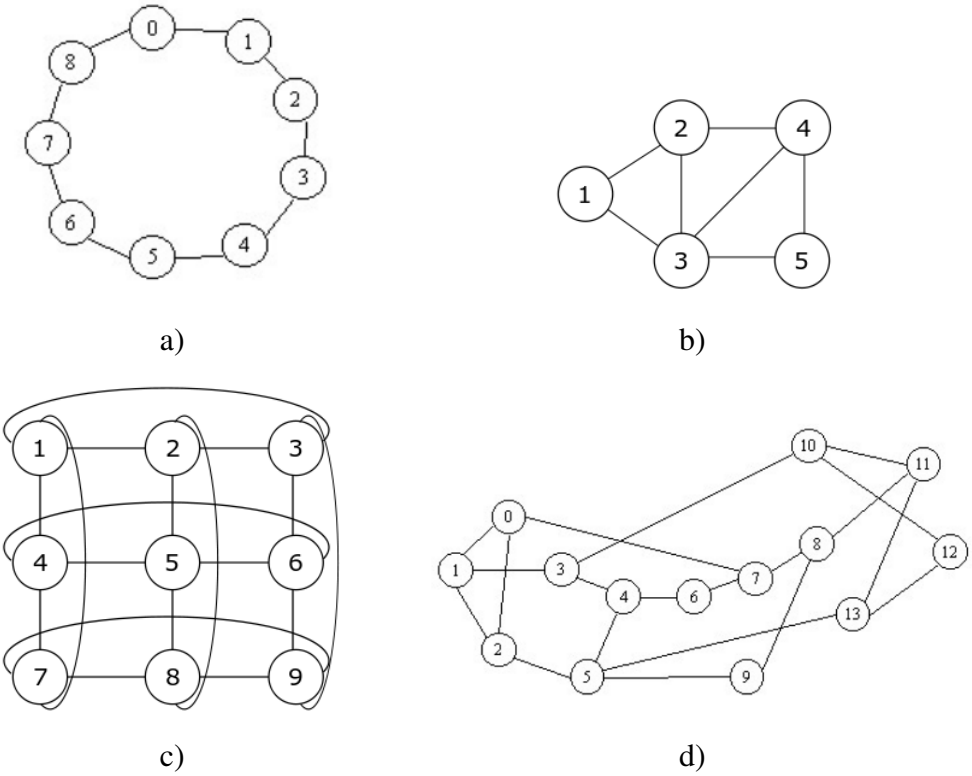


Figura 2. Topologias usadas nos experimentos: a) anel de nove nós, b) rede em malha simples com cinco nós, c) rede *mesh-torus* e d) NSFNet.

Dois cenários de análise são considerados neste artigo. No primeiro cenário, a carga oferecida à rede foi mantida fixa, com valor de 500 erlangs, e o número de comprimentos de onda variou entre 2 e 50 comprimentos de onda por fibra, num total de 24 valores distintos. No segundo cenário, manteve-se o número de comprimentos de onda com valor fixo de 10 e variou-se a carga oferecida na rede entre 10 e 500 erlangs, com incrementos de 20 erlangs, num total de 24 valores distintos de carga. Para cada valor do número de comprimentos de onda (primeiro cenário) ou de carga oferecida (segundo cenário), foram feitas 50000 solicitações de conexão.

Ao fim de cada execução é calculada a probabilidade de bloqueio da rede que serve de métrica de comparação do desempenho dos algoritmos simulados. A probabilidade de bloqueio é definida como a razão entre o número de bloqueios ocorridos sobre o número de requisições efetuadas em toda a rede.

4.1. Primeiro cenário: carga oferecida fixa e número de comprimentos de onda variando

Os resultados das simulações para esse cenário são apresentados nos gráficos de probabilidade de bloqueio em função do número de comprimentos de onda por fibra óptica dispostos na Figura 3 para a topologia em anel, na Figura 4 para a malha com 5 nós, na Figura 5 para a *mesh-torus* e na Figura 6 para a topologia da NSFNet.

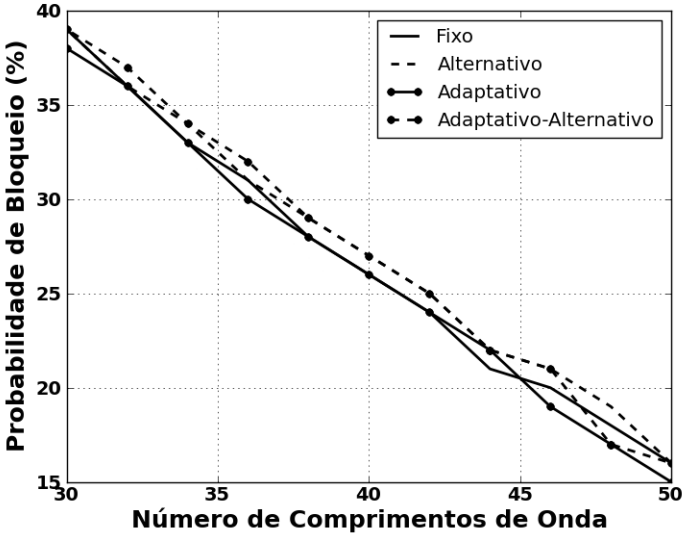


Figura 3. Probabilidade de bloqueio em função do número de comprimentos de onda na fibra para a rede em anel.

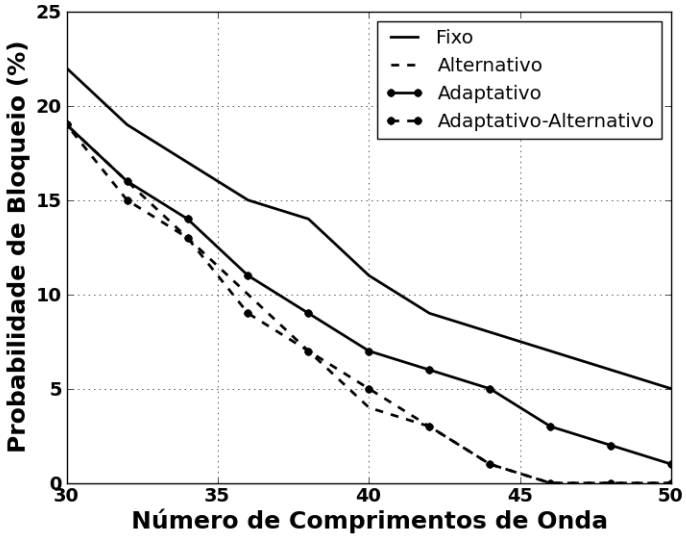


Figura 4. Probabilidade de bloqueio em função do número de comprimentos de onda na fibra para a rede com 5 nós.

Os gráficos mostram que qualquer uma das abordagens tem um desempenho superior ao roteamento fixo e também que essa diferença varia de acordo com as características topológicas da rede na qual o roteamento opera. Por exemplo, ela é significativamente menor na rede em anel, tendo em vista a baixa conectividade que esta rede tem (grau dois em cada nó) do que nas redes em malha. Já entre as outras abordagens de roteamento pode-se observar, principalmente nas topologias em malha, que o roteamento alternativo possui um desempenho igual ou superior ao adaptativo. Observa-se também que o o rote-

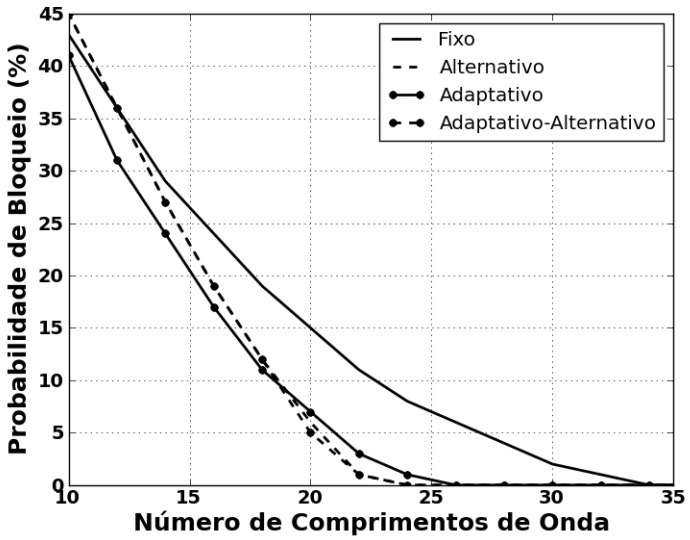


Figura 5. Probabilidade de bloqueio em função do número de comprimentos de onda na fibra para a rede *mesh-torus*.

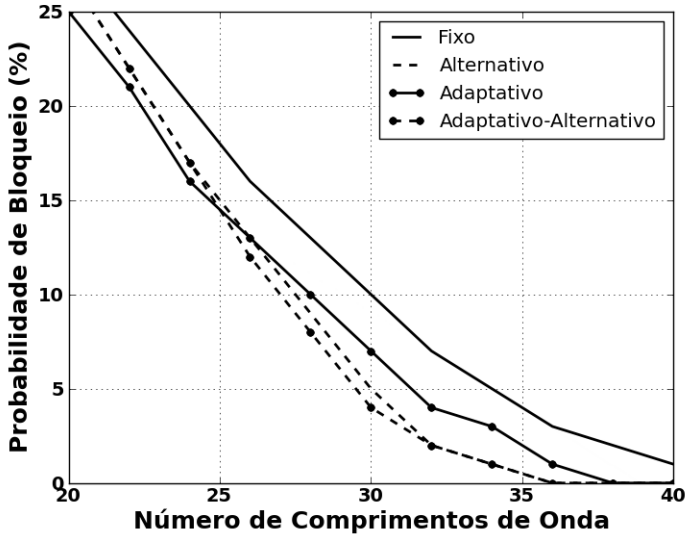


Figura 6. Probabilidade de bloqueio em função do número de comprimentos de onda na fibra para a rede NSFNet.

amento adaptativo-alternativo praticamente possui o mesmo desempenho do alternativo, apresentando uma leve superioridade em alguns casos.

É interessante observar também o número de comprimentos de onda com que a probabilidade de bloqueio se torna nula. Como esperado, esse valor muda de acordo com a topologia considerada. Quanto maior a conectividade da rede, menor o número de comprimentos de onda necessário para anular a incidência de bloqueio nas configurações consideradas. Esse comportamento pode ser exemplificado pela comparação dos resultados entre as redes estudadas. Observando-se os gráficos, pode-se ver que, nos melhores

casos, a rede em anel tem a probabilidade de bloqueio anulada com 50 comprimentos de onda por fibra; na rede de cinco nós, são necessários 47; na *mesh-torus*, 25 comprimentos de onda e na NSFNet, 37.

4.2. Segundo cenário: carga oferecida variando e número de comprimentos de onda fixo

Os resultados das simulações para esse cenário são apresentados nos gráficos de probabilidade de bloqueio em função da carga oferecida dispostos na Figura 7 para a topologia em anel, na Figura 8 para a malha com 5 nós, na Figura 9 para a *mesh-torus* e na Figura 10 para a topologia da NSFNet.

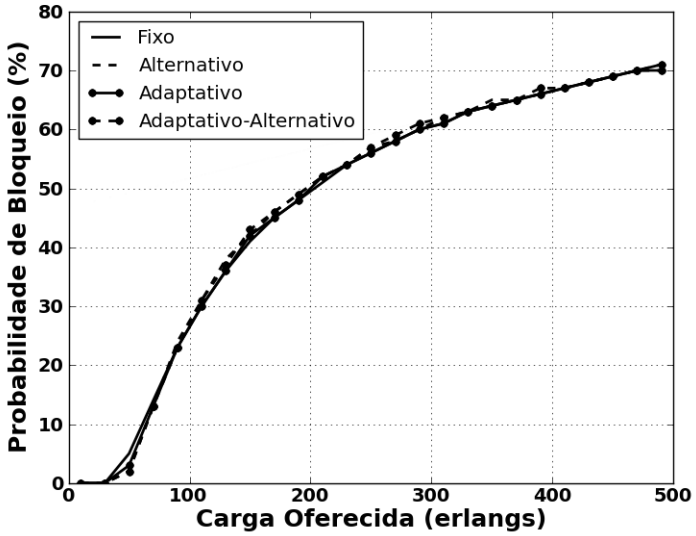


Figura 7. Probabilidade de bloqueio em função da carga oferecida para a rede em anel.

Os gráficos mostram que o uso de roteamento não-fixo, *i.e.* alternativo, adaptativo ou alternativo-adaptativo, acarreta uma diminuição na probabilidade de bloqueio para cargas baixas. Porém, a partir de um certo limiar, que varia em função da topologia, essa abordagem já não produz ganho se comparado ao roteamento fixo. Na topologia em anel, por exemplo, praticamente não há diferença de desempenho. Já na *mesh-torus* a diferença é bem mais aparente.

É interessante notar também que o desempenho do algoritmo adaptativo, destacado principalmente na *mesh-torus*, se torna superior aos demais algoritmos, fato que não ocorria no cenário anterior.

5. Conclusões

Nesse artigo, são comparadas quatro abordagens de roteamento do ponto de vista da probabilidade de bloqueio. Essa comparação é feita variando-se o número de comprimentos de onda disponíveis em cada fibra óptica mas com um valor fixo de carga oferecida na rede e, depois, variando-se a carga oferecida na rede e mantendo-se fixo o número de comprimentos de onda.

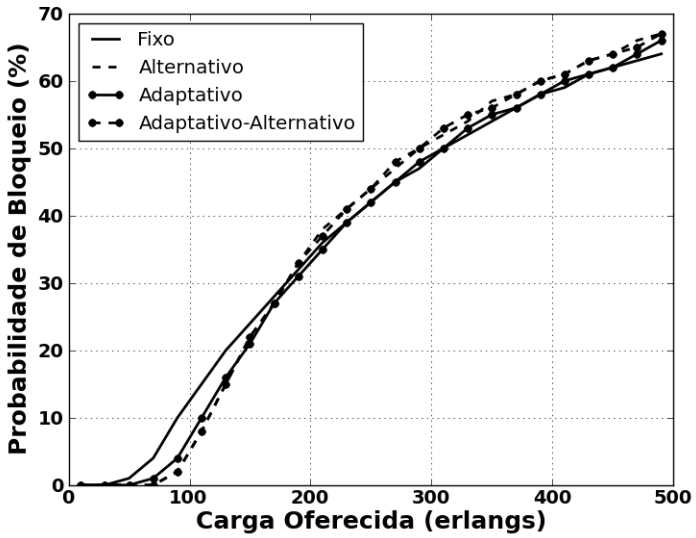


Figura 8. Probabilidade de bloqueio em função da carga oferecida para a rede com 5 nós.

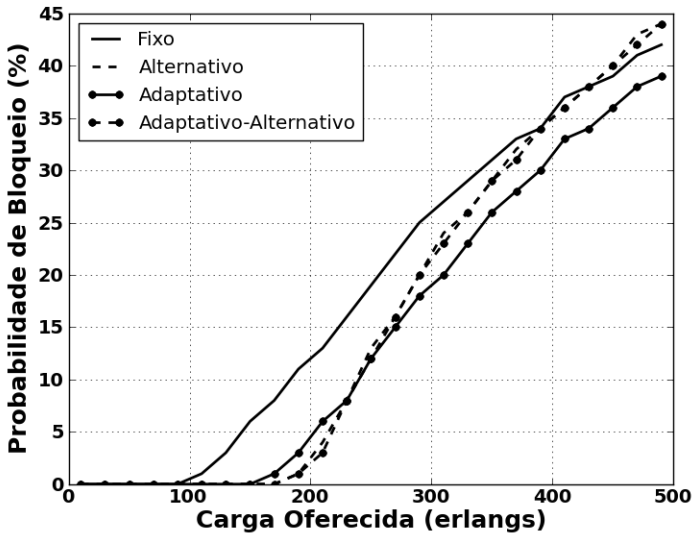


Figura 9. Probabilidade de bloqueio em função da carga oferecida para a rede *mesh-torus*.

Esses dois cenários dão uma visão mais completa do desempenho dessas abordagens de roteamento, gerando resultados que podem ajudar o operador e o projetista da rede a decidir que roteamento usar a partir das características de topologia e tráfego que esta tenha. Dentre os possíveis benefícios de uma escolha correta da abordagem de roteamento a ser utilizada se destaca a esperada diminuição no número de comprimentos de onda para se manter um dado número de bloqueios na rede. Tal característica se traduz em sistemas com menor custo de instalação e manutenção da rede. Por outro lado, se garante que a extensibilidade da rede projetada praticamente não será afetada, pois há a capacidade de se suportar um volume maior de tráfego.

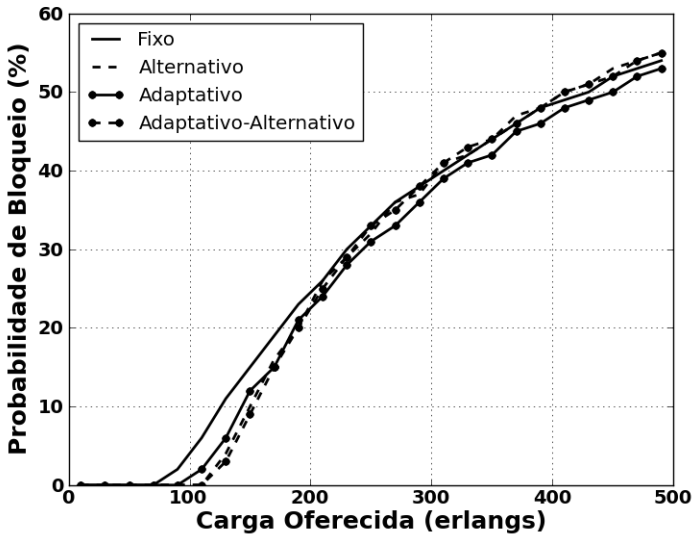


Figura 10. Probabilidade de bloqueio em função da carga oferecida para a rede NSFNet.

No primeiro cenário, no qual a carga oferecida foi mantida fixa e número de comprimentos de onda variou, observou-se que o uso de roteamento não-fixo, *i.e.* alternativo, adaptativo ou alternativo-adaptativo, leva a uma menor probabilidade de bloqueio se comparado ao uso de roteamento fixo. Observou-se também que, dependendo da topologia o número de comprimentos de onda necessários para não haver incidência de bloqueios (probabilidade de bloqueio nula) pode variar, sendo menor para topologias com maior conectividade.

No segundo cenário, no qual a carga oferecida variou e o número de comprimentos de onda foi mantido fixo, observou-se que para topologias com baixa conectividade, como o anel, não existe uma diferença significativa do algoritmo usado, mas para redes com alta conectividade, como a *mesh-torus*, essa diferença se torna mais acentuada, o que representa uma vantagem do algoritmo adaptativo sobre os demais, fato não ocorrido no cenário anterior. No entanto, a partir de um certo limiar de carga, que varia em função da topologia, praticamente não existem vantagens de nenhum algoritmo com relação aos outros.

Assim, pode-se concluir que a escolha correta da abordagem de roteamento a ser utilizada pode reduzir o número de comprimentos de onda para um dado número de bloqueios na rede. Tal característica se traduz em sistemas com menor custo de instalação e manutenção da rede. Por outro lado, se garante que a extensibilidade da rede projetada praticamente não será afetada, pois há a capacidade de se suportar um volume maior de tráfego.

Como sugestão para trabalhos futuros, pode-se fazer uso desse trabalho como ponto de partida para novas implementações, que objetivem, por exemplo, fazer uma avaliação comparativa entre os algoritmos avaliados e novas heurísticas para roteamento e para a alocação de comprimento de onda. Além disso, podem ser estabelecidos modelos matemáticos para a probabilidade de bloqueio e relações analíticas entre ela e a topologia

da rede, o que pode servir de base para a implementação de algoritmos de roteamento que tenham como parâmetro principal não só a quantidade de comprimentos de onda disponíveis no enlace, mas a quantidade de enlaces da rede, o comprimento máximo que os enlaces podem possuir para manter a qualidade de conexão e a carga oferecida na rede.

Agradecimentos

Os autores agradecem à Capes, pelo suporte financeiro ao desenvolvimento desse trabalho e ao Iecom, pela estrutura física necessária para a sua realização.

Referências

Brunato, M., Battiti, R., and Salvadori, E. (2003). Dynamic Load Balancing in WDM Networks. *Optical Networks Magazine*.

Dante, R. G. (2005). *Algoritmos de Roteamento e Atribuição de Comprimentos de Onda para as Redes Ópticas Inteligentes e Transparentes*. PhD thesis, Universidade Estadual de Campinas, Campinas, SP.

Fabry-Asztalos, T., Bhide, N., and Sivalingam, K. M. (2000). Adaptive Weight Functions for Shortest Path Routing Algorithms for Multi-Wavelength Optical WDM Networks. In *Proceedings of ICC 2000*, volume 3, pages 1330–1334, New Orleans, LA.

Fonseca, I. E. (2005). *Uma Abordagem para Aprovisionamento e Diferenciação de QoS Óptico na Presença de FWM em Redes Ópticas Transparentes*. PhD thesis, Universidade Estadual de Campinas, Campinas, SP.

Karasan, E. and Ayanoglu, E. (1998). Effects of Wavelength Routing and Selection Algorithms on Wavelength Conversion Gain in WDM Networks. In *IEEE/ACM Transactions on Networking*, volume 6, pages 186–196.

Mokhtar, A. and Azizoglu, M. (1998). Adaptive Wavelength Routing in All-Optical Networks. In *IEEE/ACM Transactions on Networking*, volume 6, pages 197–206.

Mukherjee, B. (2006). *Optical WDM Networks*. Springer, California, USA.

Ramaswami, R. and Sivarajan, K. N. (2002). *Optical Networks: A Practical Perspective*. Morgan Kaufmann Publishers, Inc., San Francisco, California, U.S.A., 2ª edition.

Rouskas, G. N. and Perros, H. G. (2002). A Tutorial on Optical Networks. Networking 2002 Tutorials - LNCS.

Wen, H., He, R., Li, L., and Wang, S. (2003). Adaptive Routing and Wavelength Assignment Algorithms in WDM Grooming Networks. In *Proceedings of ICCT2003*, volume 3.

Zang, H., Jue, J. P., and Mukherjee, B. (2000). A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks. *Optical Networks Magazine*.

XV Workshop de Gerência e Operação de Redes e Serviços

♦

Sessão Técnica 2

Aprovisionamento de Redes e Planejamento de Capacidade

Planejamento de Redes em Malha Sem Fio Lineares

Felipe Rolim e Souza e Célio V. N. Albuquerque

[1]Instituto de Computação - Universidade Federal Fluminense (UFF)

{frolim,celio}@ic.uff.br

Abstract. *Wireless mesh networks consist of mesh routers and clients, where mesh routers compose the network backbone and serve clients. The antennas associated with the routers can be omnidirectional or directional, which have a direct influence in topology construction. With this information in hand, the objective of this work is to propose and evaluate LMP, an algorithm that, given a set of coordinates organized in sequence, decides which of them will have a router installed. This decision must guarantee coverage (each coordinate must be within the coverage area of at least one mesh router) and connectivity (each mesh router must communicate with at least another one). Results obtained with real network testbeds are used to compare the required number of mesh routers, transmission rate and the average and worst signal quality with those from various techniques.*

Resumo. *Redes em malha sem fio consistem em clientes e roteadores mesh, onde os roteadores compõem o backbone da rede. As antenas associadas aos roteadores mesh podem ser omnidirecionais ou direcionais, influenciando diretamente a construção da topologia. Levando em consideração estas informações, o objetivo deste trabalho é propor e avaliar o LMP, um algoritmo que, dado um conjunto de coordenadas organizadas em sequência, decida quais devem ser escolhidas para a instalação de um roteador mesh. Esta escolha deve garantir cobertura (todos as coordenadas devem estar dentro da área de cobertura de pelo menos um roteador mesh) e conectividade (cada roteador mesh deve se comunicar com pelo menos outro). Resultados obtidos com testbeds reais servem para comparar o número mínimo de roteadores mesh necessários, taxa de transmissão, média e a pior qualidade do sinal com os de outras técnicas.*

1. Introdução

Redes em malha sem fio são compostas por roteadores e clientes *mesh*. Os roteadores normalmente são estacionários e formam o *backbone* de rede. Estes roteadores podem se comunicar com outras redes como a Internet, LANs, etc., desde que configurados como *gateways*. Uma característica das redes em malha é que os roteadores se comunicam de forma *ad-hoc* através de múltiplos saltos. Uma vantagem deste tipo de rede é a robustez. Como cada nó pode ser um potencial roteador auxiliando no encaminhamento, quanto maior a quantidade de nós, maior a quantidade de rotas alternativas na rede.

Como explicado anteriormente, as redes em malha sem fio possuem um conjunto de roteadores estacionários que constituem o *backbone* da rede. A escolha do local de posicionamento dos roteadores será o objeto de estudo deste trabalho. O tipo de antena escolhido, podendo ser direcional ou omnidirecional, possui impacto direto nesta escolha.

Ao se trabalhar com antenas direcionais, não se pode dizer que um roteador alcança outro, antes de sua antena estar alinhada em alguma direção. Isto aumenta muito a complexidade de escolha dos locais de posicionamento dos roteadores, pois implica em escolher um bom alinhamento das antenas.

Dentre as diversas topologias que redes em malha sem fio podem assumir, neste trabalho serão abordadas as redes em malha lineares. Este tipo de rede possui um conjunto pontos de interesse organizados de forma sequencial, onde o primeiro e o último atuam como *gateways*. Roteadores *mesh* podem ser instalados em qualquer ponto de interesse. Em relação ao tipo de antena, as direcionais atendem melhor a esta topologia pois a comunicação é realizada com roteadores anteriores e posteriores, não existindo a necessidade de cobertura em outras direções. A comunicação pode ser estabelecida com duas antenas direcionais, uma alinhada no sentido do roteador anterior e outra no sentido do posterior. Além disso, o alcance de antenas direcionais é maior que o de omnidirecionais. Esta configuração foi escolhida devido a um problema real de estabelecimento de comunicação ao longo de uma linha de transmissão de energia [Gerk et al. 2009]. Nesta situação, existe um conjunto de torres, organizadas sequencialmente, onde se deve escolher em quais delas serão instalados roteadores. Existem outras situações similares, como gasodutos e oleodutos, aonde redes em malha sem fio lineares podem ser aplicadas seguindo a mesma ideia. A Figura 1 apresenta a visualização em tempo real da topologia da rede em malha sem fio construída sobre a linha de transmissão de energia que liga a cidade de Machadinho à Campos Novos obtida com a ferramenta MTV - *Mesh Topology Viewer* [Valle et al. 2008].

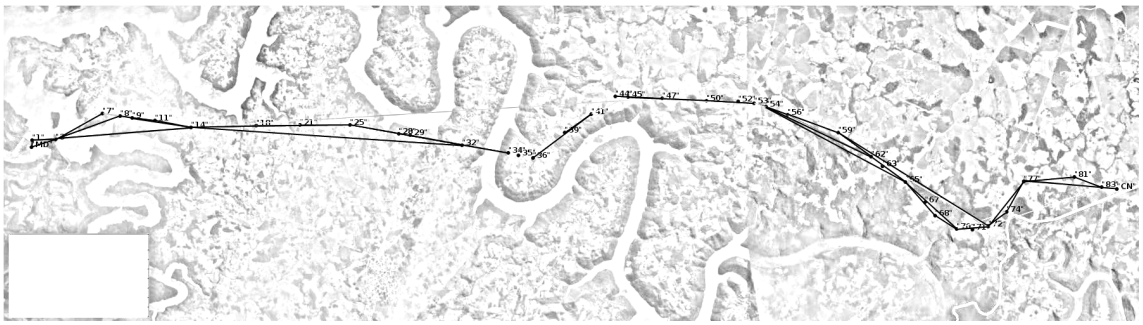


Figura 1. Visualização em tempo real da topologia da rede em malha sem fio construída sobre a linha de transmissão de energia que liga a cidade de Campos Novos à Machadinho. As linhas representam os enlaces.

Para solucionar o problema de construção do *backbone*, será proposto o algoritmo LMP (*Linear Mesh network Planning*) para o planejamento de redes em malha sem fio lineares. O objetivo principal será minimizar a quantidade de roteadores *mesh* escolhidos, porém tentando garantir que a rede possua cobertura e conectividade. Cobertura significa que todos os pontos de interesse estão pelo menos dentro da área de cobertura de pelo menos um roteador. Em relação à conectividade, um roteador deve se comunicar com pelo menos outro.

2. Trabalhos relacionados

A área de redes em malha sem fio vem recebendo diversas contribuições recentemente. Muitas destas pesquisas focam mais no desenvolvimento de protocolos do que no pla-

nejamento da rede, ao assumir que a topologia desta já é fornecida. Isto faz com que o objetivo seja otimizar, por exemplo, o roteamento.

Muitos dos trabalhos encontrados na literatura são baseados no uso de antenas omnidirecionais. A principal vantagem do uso deste tipo de antena é a facilidade de se montar um grafo, onde cada aresta representa a existência de comunicação entre dois nós. Entretanto, ao se utilizar antenas direcionais, a comunicação entre dois nós será dependente do alinhamento escolhido para cada antena. Analisando o caso de antenas omnidirecionais, temos que em [Amaldi et al. 2008], cada nó possui uma área de cobertura circular aonde o raio varia de acordo com a potência de transmissão de cada nó. Esta é normalmente a representação utilizada para antenas omnidirecionais. Utilizar esta abordagem, significa simplificar demais o modelo de propagação das antenas. Por isto, neste trabalho, serão utilizados modelos reais de propagação além da análise de obstáculos, outro fator que possui impacto direto na propagação do sinal.

Existem estudos que fazem uso de antenas direcionais para o planejamento da rede como o GPSR [Chen and Chekuri 2007]. O intuito deste é realizar o planejamento de redes em malha para regiões urbanas. Porém, neste caso, não existe a preocupação com o alinhamento das antenas para melhorar a cobertura. É definido que cada nó possui múltiplas antenas e a comunicação com outro nó acontece se existe visada direta entre eles. Diferente da solução proposta pelo GPSR, neste artigo o posicionamento das antenas é levado em consideração para que a área coberta seja a maior possível. Além do uso de redes em malha em ambientes urbanos, existe também estudos para aplicação destas em regiões rurais como pode ser visto em [Chebrolu and Raman 2007]. Este tipo de região é o que mais se assemelha ao problema de redes em malha sem fio lineares devido ao comprimento dos enlaces. Porém, a solução proposta no trabalho citado leva em consideração a utilização de diferentes tipos de antenas além das direcionais, como, por exemplo, as setoriais. Além disso, para o planejamento da solução, é levado em consideração a existência de redes locais, para as quais os enlaces de longa distância devem atender. Nenhuma dessas características fazem parte das redes em malha sem fio lineares à serem estudadas neste trabalho.

O uso eficiente de antenas direcionais também é objeto de estudo em [Kumar et al. 2006]. Os autores propõem um algoritmo para transformar uma rede em malha formada por antenas omnidirecionais em uma que utilize antenas direcionais. Para isto é necessário orientar as antenas de cada nó para que a rede continue com conectividade e a interferência seja minimizada. Porém, para garantir estas propriedades, pode ser necessário substituir uma antena omnidirecional por mais de duas antenas direcionais, valor limite para a construção das redes em malha sem fio lineares. Além disto, existe a necessidade de se possuir uma solução com antenas omnidirecionais a priori.

3. Formulação do problema

O problema de planejamento de redes em malha sem fio lineares pode ser formulado com base na teoria dos grafos. Utilizando esta abordagem, seja V uma sequência de coordenadas geográficas. A sequência V representa os vértices de um grafo direcional G. Para dois vértices $u, v \in V$, existe uma aresta partindo de u em direção a v se este é a melhor opção de alinhamento de u. Define-se como a melhor opção de alinhamento de um vértice u, outro vértice v onde a antena do primeiro, apontada para o segundo,

resulte no maior número possível de vértices dentro da área de cobertura de u. Além disso, para v ser escolhido como melhor opção, todos os vértices na sequência entre u e v devem ser cobertos (Figura 2). Isto evita que vértices fiquem fora da rede por não estarem sendo cobertos. Cada vértice poderá ter no máximo duas arestas partindo dele, uma no sentido do vértice anterior e outra no sentido do vértice posterior. Além de o vértice estar dentro da área de cobertura da antena, é necessário que não existam obstáculos impedindo a comunicação entre eles. A solução consiste em escolher um sub-grafo que conecte o primeiro ponto ao último da sequência, utilizando o menor número de vértices possível. Um exemplo de um grafo de alinhamento encontra-se na Figura 3.

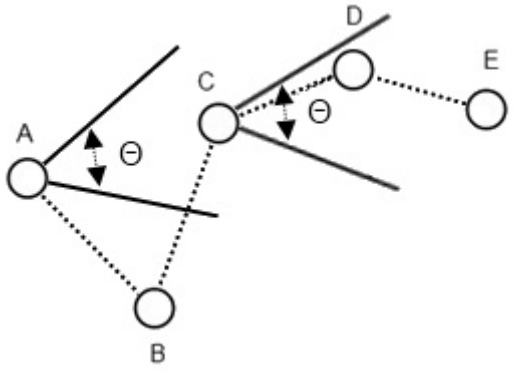


Figura 2. Utilizando uma antena direcional com ângulo de abertura θ, o vértice C alinhado com E garante a cobertura de D, porém A alinhado com C não garante a cobertura de B.

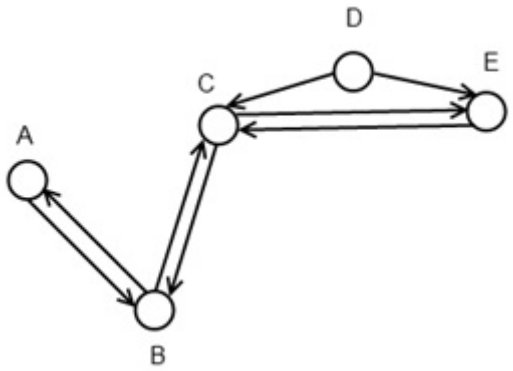


Figura 3. Exemplo de um grafo de alinhamento. Neste caso, os pares de antenas conectando A-B, B-C e C-E estão alinhadas.

4. Proposta

Nesta seção será discutido o projeto do LMP. Antes de explicar detalhadamente cada parte do algoritmo, é apresentado na Figura 4 o fluxo de execução deste. Inicialmente deve-se fornecer uma sequência de coordenadas para que o grafo de alinhamento seja construído. Esta construção requer o cálculo de área de cobertura e análise de obstáculos que irão auxiliar no processo de alinhamento das antenas. Com o grafo montado, a execução de um algoritmo de caminho mínimo irá resultar nas coordenadas que deverão ter um roteador *mesh* instalado. Pode ocorrer do algoritmo não encontrar uma solução para o conjunto de

coordenadas fornecido. A não existência da solução está relacionada a distância entre as coordenadas e a presença de obstáculos.

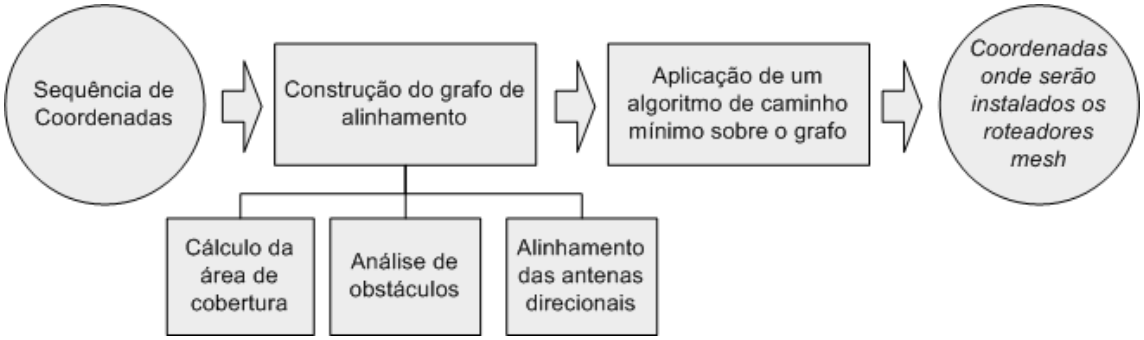


Figura 4. Diagrama exemplificando a sequência de execução do algoritmo.

Como exemplo, a solução do grafo de alinhamento da Figura 3 são os vértices A,B,C e E. Assim, estes vértices representam os locais de instalação dos roteadores *mesh* para que haja cobertura e conectividade.

4.1. Área de cobertura

Como especificado na Seção 3, a escolha do melhor vizinho de alinhamento implica em saber se uma ou mais coordenadas estão dentro de sua área de cobertura. O cálculo para determinar a cobertura ou não de uma coordenada é especificado pela equação do *Link Budget*. Esta equação fornece o sinal recebido utilizando basicamente a soma da potência de saída com os ganhos e perdas relativas as antenas tanto do transmissor quanto do receptor. A fórmula a ser utilizada será a seguinte:

$$PRX = PTX + GTX - LTX - LFS - LM + GRX - LRX, \quad (1)$$

onde PTX e GTX representam, respectivamente, a potência de saída e o ganho da antena enquanto as variáveis LTX, LM indicam as perdas relativas a cabos e conexões e a fatores diversos. A variável LFS representa o resultado da equação conhecida como *Free-space Path Loss*, que indica a perda sofrida pela atenuação do sinal devido a distância entre duas antenas. A equação utilizada é a seguinte:

$$LFS = 32,45 + 20 * log(FREQ) + 20 * log(DIST), \quad (2)$$

onde FREQ representa a frequência em Mhz e DIST a distância em quilômetros. Todos os valores citados até aqui estão relacionados ao transmissor. Aqueles representados por GRX e LRX indicam o ganho da antena e as perdas do receptor. Estas duas variáveis são utilizadas apenas quando se calcula o *Link Budget* para o candidato a melhor vizinho. Isto ocorre porque se este candidato for escolhido para a instalação de um roteador, ele receberá uma antena já conhecida. Para as coordenadas localizadas entre a origem e seu melhor vizinho, as variáveis relacionadas ao receptor são ignoradas. Isto porque não se sabe a priori as antenas dos dispositivos que utilizarão a rede. Porém, a omissão destes dois parâmetros não traz consequências negativas, pois o dispositivo que utilizará a rede terá o sinal recebido somado ao ganho de sua antena.

Como especificado, um dos parâmetros é o ganho da antena. Quando se utiliza antenas direcionais, este valor depende do ângulo formado entre a antena e a coordenada a

ser analisada, pois o padrão de irradiação horizontal não é circular como nas antenas omnidirecionais. Para determinar este padrão de irradiação, considera-se, para cada ângulo horizontal e vertical com intervalos de 1º, a perda relativa ao ângulo de ganho máximo (0º)[1].

O resultado da equação do *Link Budget* será comparado a um limiar estabelecido de acordo com a sensibilidade do rádio. Caso o resultado esteja abaixo do limiar, é determinado que a coordenada está fora da área de cobertura da antena.

4.2. Análise de obstáculos

Outro fator, descrito na formulação do problema, para existência de comunicação é a não presença de obstáculos. Para determinar se os obstáculos irão permitir ou não a comunicação, será utilizada a equação da zona de Fresnel. A zona de Fresnel é um dos elipsoides concêntricos entre dois pontos de um sistema de rádio (Figura 5). Para que uma transmissão de rádio seja possível, é necessário que uma porcentagem deste elipsoide não esteja obstruída. O valor padrão desta porcentagem é de 60%. A Equação 3 apresenta o cálculo do raio da zona de Fresnel. O parâmetro PORC representa a porcentagem da zona de Fresnel que precisa estar desobstruída e FREQ indica a frequência das antenas. Os valores D1 e D2 são, respectivamente, a distância do obstáculo até a primeira antena e a distância até a segunda antena. Através deste raio, e conhecendo a altura em que as antenas estão instaladas, é possível definir a elevação máxima, em relação ao nível do mar, que permita a comunicação.

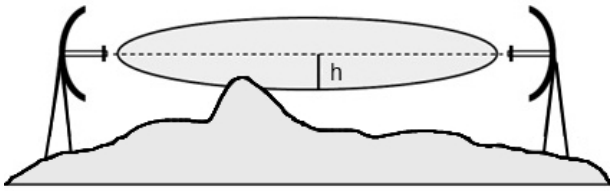


Figura 5. Na zona de Fresnel, o raio h do elipsoide está relacionado a frequência de transmissão e a distância.

$$RAIO = 17.31 * \sqrt{\frac{PORC * D1 * D2}{FREQ * (D1 + D2)}} \tag{3}$$

Para descobrir os obstáculos existentes entre duas coordenadas geográficas, utilizou-se uma base de dados contendo as elevações geográficas da região em que as coordenadas de entrada estão localizadas. Com a equação e a base de dados definidas, para saber se existem obstáculos que possam impedir a comunicação entre duas coordenadas, o LMP analisa todas aquelas intermediárias entre elas, existentes na base de dados, comparando com a elevação máxima calculada pela zona de Fresnel. Caso o valor encontrado na base de dados seja superior ao calculado, a comunicação não poderá ocorrer.

Caso não existam informações de elevação em determinada região, o algoritmo irá considerar como obstáculo a elevação das coordenadas intermediárias as duas sendo analisadas. Desta forma, torna-se obrigatório, para correto funcionamento do algoritmo, fornecer a elevação de todas as coordenadas.

[1]O padrão de irradiação da antena deve ser fornecido pelo fabricante.

LMP(V, $Limiar$)
1: $G \leftarrow Coordenadas(V)$
2: **for** cada coordenada $i \in V$ **do**
3: $EscolheMelhorVizinho(i, G, Limiar, Posterior)$
4: $EscolheMelhorVizinho(i, G, Limiar, Anterior)$
5: **end for**
6: $Primeira \leftarrow PrimeiraCoordenada(V)$
7: $Última \leftarrow ÚltimaCoordenada(V)$
8: $R1 \leftarrow CaminhoMínimo(G, Primeira, Última)$
9: $R2 \leftarrow CaminhoMínimo(G, Última, Primeira)$
10: $R \leftarrow min(R1, R2)$

Figura 6. Pseudocódigo do funcionamento básico do algoritmo para antenas direcionais.

4.3. Construção do grafo de alinhamento

Como visto na Figura 4 o primeiro passo é a construção do grafo de alinhamento. Para isto, é considerado que todas as coordenadas são possíveis locais de instalação de roteadores *mesh*. Isto significa que a coordenada, além do roteador, irá receber um par de antenas e um rádio. Com esta consideração inicial, é possível construir o grafo de alinhamento como descrito na Seção 3. A construção deste requer que as antenas de cada coordenada estejam alinhadas com seus melhores vizinhos. Com o grafo montado, a execução de um algoritmo de caminho mínimo resultará em uma solução indicando a quantidade mínima de coordenadas necessárias onde deverão ser efetivamente instalados os roteadores *mesh*. Dependendo de qual ponto se inicia a execução do algoritmo de caminho mínimo (primeiro ou último), diferentes resultados podem ser obtidos. Isto porque v pode ser o melhor vizinho de u, porém u pode não ser o melhor vizinho de v. Dentre os dois grafos é escolhido aquele cujo caminho mínimo possua a menor quantidade de roteadores.

Na Figura 6 este procedimento está apresentado sob a forma de pseudocódigo. O procedimento necessita como parâmetro de entrada um conjunto de coordenadas V e o limiar a ser utilizado pela equação do *Link Budget*. Além deste parâmetro será utilizado um grafo direcional G que inicialmente possui como vértices as coordenadas de V (linha 1). Para cada coordenada $i \in V$, o procedimento que escolhe o melhor vizinho irá adicionar uma aresta em G conectando i aos seus melhores vizinhos (um no sentido anterior e outra no posterior) (linhas 3 e 4). Finalmente, a execução de um algoritmo de caminho mínimo sobre G irá resultar nos conjuntos $R1$ e $R2$ (linhas 8 e 9). O conjunto $R1$ possui as coordenadas do caminho mínimo partindo da primeira para a última coordenada de V, enquanto o conjunto $R2$ possui as coordenadas do caminho no sentido contrário. Dentre estes dois conjuntos, é escolhido aquele que possui o menor número de elementos (linha 10), resultando no conjunto R que possuirá as coordenadas indicando os locais de instalação dos roteadores *mesh*.

A grande dificuldade está na escolha do melhor vizinho. Como já definido anteriormente, o melhor vizinho v de u é aquele que, ao ter a antena de u direcionada para ele, possua o maior número de outras coordenadas dentro da área de cobertura. Deve-se ressaltar que caso uma das coordenadas intermediárias entre u e v não esteja sendo coberta, v

EscolheMelhorVizinho(i, G, $Limiar$, $Sentido$)

```
 1: if Sentido = Posterior then
 2:     Vizinho ← i + 1
 3: else
 4:     Vizinho ← i − 1
 5: end if
 6: Max ← 0
 7: Contador ← AnalisaCobertura(i, Vizinho, Limiar)
 8: while Contador > 0 do
 9:     if (Contador > Max) e (ExisteObstáculo(i, Vizinho) = falso) then
10:         Max ← Contador
11:         MelhorVizinho ← Vizinho
12:     end if
13:     if Sentido = Posterior then
14:         Vizinho ← Vizinho + 1
15:     else
16:         Vizinho ← Vizinho − 1
17:     end if
18:     Contador ← AnalisaCobertura(i, Vizinho, Limiar)
19: end while
20: InsereAresta(G, i, MelhorVizinho)
```

Figura 7. Pseudocódigo do funcionamento do algoritmo de escolha do melhor vizinho.

não será considerado o melhor vizinho (Figura 2). O pseudocódigo do algoritmo de escolha do melhor vizinho pode ser visto na Figura 7. Primeiramente, é preciso saber quem é o primeiro vizinho da coordenada i. Esta informação é fornecida pelo parâmetro $Sentido$, que indica se os vizinhos posteriores ou anteriores serão analisados. Assim, pode-se definir o primeiro vizinho de i como sendo o próximo (linha 2) ou o anterior (linha 4). Com o vizinho definido, deve-se determinar se ele é a melhor opção de alinhamento. Para isso, a quantidade de coordenadas cobertas quando i tem sua antena alinhada para $Vizinho$, calculada pela função $AnalisaCobertura$ (linha 7), deve ser maior que um máximo estipulado inicialmente com valor 0 (linha 6). Caso este contador seja maior que o máximo e não existe nenhum obstáculo entre i e $Vizinho$ (linha 9), este passa a ser considerado o melhor vizinho de i (linha 11) e a variável Max passa a possuir o valor calculado pela função $AnalisaCobertura$ (linha 10). A função que informa a existência de obstáculos, utiliza o procedimento descrito na Subseção 4.2. Em seguida, é necessário continuar analisando os outros vizinhos de i, o que é realizado incrementado ou decrementando a variável $Vizinho$ (linha 13) e repetindo o processo descrito até que a quantidade de coordenadas intermediárias seja igual a 0, ou seja, quando não for possível estabelecer uma comunicação entre i e $Vizinho$. Definido o melhor vizinho, é criada uma aresta em G ligando i a $MelhorVizinho$ (linha 20).

A Figura 8 apresenta o pseudocódigo da função $AnalisaCobertura$. O objetivo desta função é contar, através do cálculo do ***LinkBudget***, a quantidade de coordenadas cobertas resultante do alinhamento da antena de uma coordenada i para um de seus vizi-

```
AnalisaCobertura(i, Vizinho, Limiar)
 1: Contador ← 0
 2: if LinkBudget(i, Vizinho) > Limiar then
 3:    Contador ← Contador + 1
 4:    for cada ponto intermediário j entre i e Vizinho do
 5:       if LinkBudget(i, j) > Limiar then
 6:          Contador ← Contador + 1
 7:       else
 8:          Contador ← 0
 9:          Termina repetição pois j não está sendo coberto
10:       end if
11:    end for
12: end if
13: return Contador
```

Figura 8. Pseudocódigo para contagem de coordenadas dentro da área de cobertura.

nhos. A quantidade de coordenadas cobertas será armazenada na variável $Contador$ que possui seu valor inicial igual a 0 (linha 1). O primeiro passo é analisar se existe um sinal mínimo, estipulado pela variável $Limiar$, chegando em $Vizinho$ (linha 2). Em caso positivo, as coordenadas intermediárias entre i e $Vizinho$ serão analisadas (linha 4). Caso o cálculo do *Link Budget* seja superior a $Limiar$, é considerado que a coordenada está sendo coberta, e $Contador$ é incrementado em uma unidade (linha 6). Em caso contrário, a restrição de cobertura está sendo violada, pois todas as coordenadas intermediárias devem ser cobertas. Desta forma, a função deverá retornar o valor 0 (linha 8) e não há a necessidade de se analisar as outras coordenadas (linha 9).

5. Resultados

Nesta seção serão apresentadas as soluções encontradas pelo algoritmo LMP para dois conjuntos de coordenadas reais. Ambos os conjuntos consistem em linhas de transmissão de energia fornecidas pela empresa TBE. A primeira, que liga a cidade de Machadinho a Campos Novos, possui 85 torres totalizando, aproximadamente, 50 quilômetros de extensão. Três soluções manuais já haviam sido compostas para este conjunto por um especialista em projeto de redes sem fio formado em engenharia de telecomunicações. A primeira teve como objetivo minimizar a quantidade de roteadores, enquanto as outras duas introduziram redundância à primeira solução. A solução com a maior quantidade de roteadores (maior redundância) foi aplicada a linha de transmissão e encontra-se operacional. Para avaliar o LMP, o resultado deste será comparado à primeira solução manual, já que ambas possuem o objetivo de minimizar a quantidade de roteadores. Uma comparação é viável, pois a rede em operação é uma variante da solução manual citada e ambas foram construídas utilizando o mesmo procedimento. A segunda linha de transmissão liga a cidade de Açaílandia a Imperatriz e possui 128 torres em aproximadamente 62 quilômetros de extensão. Para este conjunto não existe solução manual.

Em relação aos parâmetros para a equação do *Link Budget*, serão utilizadas as mesmas informações das antenas direcionais e roteadores que se encontram na rede em

funcionamento. Os valores são: 20 dBm para a potência de saída, 24 dBi para o ganho da antena direcional, 2,4 Ghz para a frequência e 5 dB de perda devido a cabos e conectores. O parâmetro relativo a perdas diversas não será utilizado. Deve-se ressaltar que o ganho da antena mencionado se refere ao ângulo de ganho máximo.

A base de dados de elevações, utilizada para análise de obstáculos, foi obtida através do *site* de monitoramento por satélite da EMBRAPA[2]. Esta base de dados está codificada em um formato de arquivo conhecido como GeoTIFF, utilizado para armazenamento de informações geográficas.

5.1. Métricas

Para analisar os resultados obtidos, métricas de comparação devem ser definidas. Nem sempre os melhores valores de uma métrica, significam os melhores valores de outra. Podemos citar como exemplo a relação entre a potência do sinal e a interferência intra-fluxo. Esta interferência é causada pelo sinal recebido de transmissões de outros nós que não fazem parte do enlace em questão (Figura 9). Quanto mais roteadores forem adicionados, maior será a potência do sinal recebido devido a proximidade entre eles, porém existirá uma maior interferência intra-fluxo.

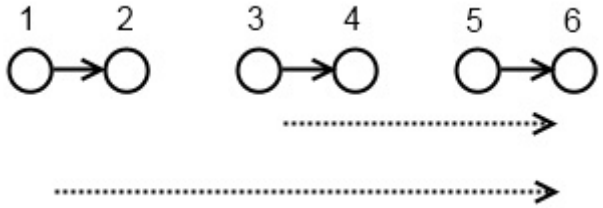


Figura 9. A comunicação entre os pontos 5 e 6 recebe os sinais das comunicações entre os pares 1,2 e 3,4.

Para avaliar o LMP, serão utilizadas cinco métricas: quantidade de roteadores, potência do sinal médio, menor potência de sinal recebida, interferência intra-fluxo e a taxa máxima de transferência no pior enlace. A quantidade de roteadores é a métrica que o LMP objetiva minimizar respeitando o limiar estabelecido. A potência do sinal médio recebido é calculada somando, para cada par de antenas diretamente alinhadas, a potência do sinal entre elas e dividindo este somatório pela quantidade de pares. A menor potência de sinal recebida é o valor do sinal mais fraco formado por um par de antenas diretamente alinhadas. A interferência intra-fluxo é a métrica mais difícil de ser calculada. Isto, porque não se pode estabelecer a priori quais enlaces serão formados e que transmissões simultâneas ocorrerão. Variáveis diversas, como o algoritmo de roteamento, implicam na formação da topologia. O ideal é que o enlace seja formado por um par de antenas diretamente alinhadas. Para que um comparativo seja estabelecido, será necessário definir a formação dos enlaces. Como o objetivo do algoritmo é construir uma solução a fim de minimizar a quantidade de roteadores, a redundância não é um fator levado em consideração. Desta forma, a incidência de redundâncias será pequena, o que torna viável considerar os pares de antenas diretamente alinhadas como um enlace. Com esta abordagem, a interferência intra-fluxo será analisada de duas maneiras: através da média da

[2]www.relevobr.cnpm.embrapa.br

interferência na rede e comparando a interferência mais forte sofrida em um enlace. Já que as métricas de qualidade do sinal e interferência foram definidas, é possível estabelecer a relação sinal-ruído e com isto estimar a taxa de transferência. Para a comparação das soluções, será estimada a taxa máxima no enlace que possui o sinal mais fraco.

Como descrito anteriormente, a interferência intra-fluxo é causada pela potência do sinal das comunicações dos outros enlaces da rede. Para calcular esta interferência, será estabelecido um cenário de pior caso, ou seja, será considerado que todas comunicações possíveis anteriores ao receptor estejam ativas. Na Figura 9 a interferência recebida por 6 será a causada pelas transmissões de 1 para 2 e de 3 para 4. Este é um cenário de pior caso, pois nem sempre todas as comunicações possíveis ocorrem simultaneamente.

Outra métrica definida foi a taxa máxima de transferência no pior enlace da rede. Para determinar qual taxa será viável para o enlace, será analisada a taxa de erro de pacote (*Packet Error Rate - PER*) para a relação sinal-ruído. Esta taxa de perda será calculada de acordo com a seguinte equação:

$$PER = \frac{1 - erf(\frac{SNR-a}{b\sqrt{2}})}{2}, \tag{4}$$

aonde SNR é a relação sinal-ruído e $erf(x)$ é a *Função Erro* [Passos and Albuquerque 2010]. Os parâmetros a e b são constantes para determinada combinação de taxa de transferência e tamanho de quadro. Tanto a função apresentada quanto os parâmetros a e b foram definidos em [Passos and Albuquerque 2010]. Será considerada a taxa máxima de transferência, a maior destas que possua um $PER \leq 1\%$.

5.2. Comparativo entre a solução manual e a do LMP

Dentre as três soluções manuais existentes, será utilizada aquela que possui o mesmo objetivo do LMP: minimizar a quantidade de roteadores. Da mesma forma que o LMP, a solução manual também foi construída com a ideia de se respeitar um valor mínimo de qualidade de sinal. O valor utilizado para esta solução foi de -75 dBm, que também será utilizado como limiar para o LMP. As métricas definidas anteriormente foram calculadas para ambas as soluções e um comparativo pode ser visto na Tabela 1.

Tabela 1. Comparação das métricas entre solução manual e do algoritmo LMP.

	LMP	**Manual**
Quantidade de Roteadores	10	16
Sinal Médio	-54,15 $\pm$ 3,33 dBm	-46,84 $\pm$ 9,60 dBm
Pior Sinal	-56,87 dBm	-58,07 dBm
Média da Interferência	-65,73 $\pm$ 1,15 dBm	-61,97 $\pm$ 4,97 dBm
Interferência Mais Forte	-64,06 dBm	-52,22 dBm
Taxa Máxima no Pior Enlace	12 Mbps	6 Mbps

Como se pode analisar pelos resultados das métricas, o LMP encontrou uma solução que garante as mesmas propriedades da manual utilizando uma quantidade de roteadores inferior. Como era de se esperar a média do sinal da solução com mais roteadores foi maior que a apresentada pelo LMP. Isto porque a maior quantidade de roteadores

acaba implicando em uma proximidade maior entre eles, resultando em áreas com uma qualidade de sinal elevada. Além da média dos sinais, foi calculado o desvio padrão para esses valores. Para a solução do LMP o valor do desvio padrão foi de 3,33 dBm, enquanto a solução manual apresentou o valor de 9,60 dBm. Apesar da solução manual apresentar uma média superior, a discrepância entre os sinais é maior. Esta discrepância pode ser observada pelo pior sinal da solução manual que é bem inferior a média, enquanto na solução do LMP a diferença entre os dois valores é pequena.

Com os resultados da interferência, pode-se perceber o impacto que uma métrica possui sobre a outra. A maior quantidade de roteadores da solução manual resultou em uma qualidade de sinal média superior (apesar de não uniformemente distribuída), mas trouxe consigo uma média de interferência mais elevada. O desvio padrão sobre as interferências resultou em 1,15 dBm para a solução do LMP e 4,97 dBm para a manual. É possível observar que além de inferior, a interferência do LMP é mais uniforme. Novamente, esta diferença pode ser observada pelos valores de interferência mais forte calculada para ambas as soluções.

Outra métrica definida presente na Tabela 1 é a taxa máxima de transmissão no pior enlace da rede. Para esta métrica, foi calculada para cada taxa de transmissão disponível a taxa de erro de pacote (Eq. 4) e escolhido a maior taxa de transferência onde $PER \leq 1\%$. O tamanho do quadro utilizado foi o de 1500 bytes. Pelos resultados obtidos, a taxa máxima no pior enlace da rede foi maior para o LMP (12 Mbps) do que a encontrada para a solução manual (6 Mbps). Isto se deve a uma menor interferência e a um sinal mais forte, resultando em uma relação sinal-ruído superior.

5.3. Algoritmo por distância

Devido a escassez de soluções manuais, o LMP será comparado com outras técnicas simples de escolha do local de instalação dos roteadores. Uma forma de realizar esta escolha é através do comprimento do enlace. Sabendo o alcance da antena, escolhe-se o próximo local como sendo aquele cuja distância seja a máxima dentro da área de cobertura. Foram executadas instâncias deste algoritmo por distância com diferentes comprimentos. A linha de transmissão e a solução do LMP a serem utilizadas serão as mesmas apresentadas no comparativo com a solução manual. A Tabela 2 apresenta os valores das métricas para as soluções encontradas.

Tabela 2. Apresentação das métricas do algoritmo por distância.

	LMP	**5Km**	**5,5Km**	**6Km**
Quantidade de Roteadores	10	9	8	7
Sinal Médio	-54,15 dBm	-54,98 dBm	-56,21 dBm	-58,02 dBm
Pior Sinal	-56,87 dBm	-56,68 dBm	-57,67 dBm	-58,34 dBm
Média da Interferência	-65,73 dBm	-66,49 dBm	-66,89 dBm	-68,68 dBm
Interferência Mais Forte	-64,06 dBm	-64,39 dBm	-64,24 dBm	-67,75 dBm
Coordenadas não cobertas	0	1	9	4

Apesar das soluções do algoritmo por distância apresentarem resultados similares ou até mesmo superiores ao do LMP, este apresenta uma característica que o primeiro não possui: a garantia de cobertura. Para determinar se todos os pontos entre dois roteadores estão sendo cobertos, cada um deverá ter um sinal, calculado através do

Link Budget, superior ao limiar para pelo menos um dos roteadores e a comunicação deve estar livre de obstáculos. Pelos resultados apresentados, pode-se perceber que o correto posicionamento dos roteadores é fundamental para garantir a cobertura de todas as coordenadas. Esta afirmativa é válida já que com a distância de 6 quilômetros entre cada roteador, a quantidade de coordenadas cobertas foi superior comparada a distância de 5,5 quilômetros, apesar desta solução possuir uma quantidade maior de roteadores. Como o LMP realiza análise de obstáculos e garantia de qualidade de sinal, impedindo comunicações que deixem pontos descobertos, a cobertura é total.

5.4. Variando o limiar do LMP

Nesta seção, será utilizada a segunda linha de transmissão citada (Açaílandia-Imperatriz) para uma comparação das soluções do LMP para diferentes valores de limiar. Como já explicado anteriormente, este limiar está relacionado a sensibilidade do rádio a ser utilizado na construção da rede. Assim, dependendo de suas características, soluções serão construídas de acordo. As métricas das soluções para diferentes valores de limiar estão localizadas na Tabela 3.

Tabela 3. Comparação das métricas para diferentes valores de limiar.

	-70 dBm	**-75 dBm**	**-80 dBm**	**-85 dBm**
Quantidade de Roteadores	24	17	10	6
Sinal Médio	-48,68 dBm	-51,45 dBm	-55,44 dBm	-60,15 dBm
Pior Sinal	-52,67 dBm	-56,63 dBm	-61,62 dBm	-66,16 dBm
Média da Interferência	-58,49 dBm	-62,55 dBm	-70,46 dBm	-80,49 dBm
Interferência Mais Forte	-55,03 dBm	-57,13 dBm	-64,27 dBm	-74,59 dBm

Como era de se esperar, quanto menor a sensibilidade, maior a quantidade de roteadores *mesh* que a rede possuirá. Uma maior quantidade traz, porém, um maior nível de interferência. Assim como os resultados apresentados na Subseção 5.2, a solução encontrada pelo algoritmo tende a ser uniforme, já que o pior sinal encontrado para cada um dos limiares é bem próximo da média do sinal. O mesmo pode ser dito sobre a interferência. Os valores mais altos encontrados não se afastam muito da média.

6. Conclusões

Neste artigo foi discutido o planejamento de redes em malha sem fio lineares e proposto o algoritmo LMP cujo objetivo é minimizar o número de roteadores *mesh* instalados. A escolha do local de instalação dos roteadores deve garantir cobertura e conectividade para toda a rede. Como o foco do LMP é a utilização de antenas direcionais, o alinhamento destas é fator fundamental para garantir as duas propriedades apresentadas. Com o intuito de escolher o alinhamento das antenas, foi desenvolvida a heurística de escolha do melhor vizinho. Um outro fator que influencia o alinhamento das antenas é a presença de obstáculos. Para solucionar o problema de como determinar a existência de obstáculos, foi utilizado uma base de dados contendo, para as coordenadas de uma região, a elevação de cada uma.

Para avaliar o resultado obtido com o LMP, este foi comparado com uma solução manual projetada para a rede em malha sem fio em operação sobre a linha de transmissão que liga Campos Novos à Machadinho assim como uma outra técnica simples baseada

em distância. Para o primeiro caso, o LMP conseguiu construir uma solução que utilizou menos roteadores e obteve uma menor interferência e uma maior taxa de transmissão no pior enlace. Em relação à técnica por distância, foi mostrado que esta não garante a cobertura total dos pontos, o que é alcançado pelo LMP. A segunda linha de transmissão (Açailândia-Imperatriz) foi utilizada para comparar as soluções encontradas pelo LMP para diferentes valores de limiar.

A principal vantagem do algoritmo proposto é a utilização de informações reais para escolha da solução. A área de cobertura é calculada de acordo com dados reais da antena e do rádio, e não apenas uma aproximação por distância. Os dados de entrada do algoritmo são coordenadas em latitude e longitude, e estas informações permitem ao algoritmo, com auxílio de uma base de dados de elevações, localizar os obstáculos existente entre duas coordenadas. Dadas estas informações, a solução é construída considerando o cenário real e as restrições de cobertura e conectividade.

Referências

Amaldi, E., Capone, A., Cesana, M., Filippini, I., and Malucelli, F. (2008). Optimization models and methods for planning wireless mesh networks. *Comput. Netw.*, 52(11):2159–2171.

Chebrolu, K. and Raman, B. (2007). Fractel: a fresh perspective on (rural) mesh networks. In *NSDR '07: Proceedings of the 2007 workshop on Networked systems for developing regions*, pages 1–6, New York, NY, USA. ACM.

Chen, C. and Chekuri, R. (2007). Urban wireless mesh network planning: The case of directional antennas. Technical Report UIUCDCS-R-2007-2874, University of Illinois at Urbana-Champaign Computer Science Department.

Gerk, L., Passos, D., Muchaluat-Saade, D. C., and Albuquerque, C. (2009). Infraestrutura de comunicação em malha sem fio para supervisão e controle de sistemas de transmissão de energia. In *Espaço Energia*, volume 10, pages 1–10.

Kumar, U., Gupta, H., and Das, S. (2006). A topology control approach to using directional antennas in wireless mesh networks. volume 9, pages 4083 –4088.

Passos, D. and Albuquerque, C. (2010). Implementação e análise prática de desempenho do mecanismo mara em redes em malha sem fio. In *Simpósio Brasileiro de Redes de Computadores (SBRC 2010)*.

Valle, R., Passos, D., Albuquerque, C., and Muchaluat-Saade, D. C. (2008). Mesh topology viewer (mtv): an svg-based interactive mesh network topology visualization tool. In *IEEE Symposium on Computers and Communications (ISCC 2008)*.

Proposta de Método para Engenharia de Tráfego em Redes *Mesh*

Andrey Juliano Fischer, Edgard Jamhour

Pontifícia Universidade Católica do Paraná – PUCPR
Rua Imaculada Conceição, 1115 – Prado Velho – Curitiba – PR – CEP: 80215-901

Programa de Pós-Graduação em Informática Aplicada – PPGIA
{andrey.fischer, jamhour}@ppgia.pucpr.br

Abstract. *This paper proposes a method for providing traffic engineering on wireless mesh networks based on IEEE 802.11. The method determines the maximum channel capacity by using the concepts of collision domain, considering the hidden nodes, the spatial reuse, and the channel theoretical capacity. As the maximum channel capacity depends on the quantity of traffic and the path routes, this work proposes the use of optimization methods to choose the best routes to be used by the traffic demands in order to offer the best network provisioning without exceeding the maximum channel capacity.*

Resumo. *Neste trabalho propomos um método para prover engenharia de tráfego às redes mesh sem fio baseadas no padrão IEEE 802.11. O método determina a capacidade máxima de transmissão de uma rede mesh usando os conceitos de domínio de colisão, considerando os nós escondidos, o reuso espacial e a capacidade teórica do canal. Como a capacidade máxima de transmissão é afetada pela quantidade de tráfego e caminho utilizado na rede, este artigo propõe o uso de métodos de otimização para escolha dos melhores caminhos a serem utilizados pelas demandas de tráfego para oferecer o melhor provisionamento da rede sem exceder a capacidade máxima do canal.*

1. Introdução

Atualmente, tecnologias como ADSL (*Asymmetric Digital Subscriber Line*), PON (*Passive Optical Network*) e *cable modem* apresentam-se como soluções para a construção de redes de acesso para *backbones* metropolitanos. Porém, sua utilização torna-se inviável para suprir acesso às zonas metropolitanas de menor poder aquisitivo ou com pouca densidade demográfica, pois implicam em elevados custos de implantação, manutenção e expansão, motivando a pesquisa de tecnologias alternativas de baixo custo que tenham potencial para atender a esse tipo de demanda.

Entre as tecnologias de rede alternativas podemos citar o Wi-Fi (*Wireless Fidelity*), padrão IEEE 802.11, que apesar de apresentar baixo custo de implantação, manutenção e expansão, é mais vulnerável à interferências por utilizar frequências de operação não licenciadas, como 2.4GHz e 5.8GHz. Por essas razões, o dimensionamento da capacidade, a implantação de mecanismos para controle de qualidade de serviço e o balanceamento de carga em redes Wi-Fi constituem um tópico com grande potencial de pesquisa e desenvolvimento.

Existem muitos trabalhos relacionados à pesquisa da capacidade de redes *ad-hoc* como [Gupta e Kumar 2000], [Couto *et al.* 2001] e [Jain *et al.* 2003], porém os resultados apresentados são inadequados as WMN (*Wireless Mesh Networks*) devido às suas particularidades. Conforme [Aoun e Boutaba 2006], pode-se dizer que ao contrário de uma rede *ad-hoc*, uma WMN apresenta topologia estável, exceto para eventuais falhas e adição de novos nós, e que praticamente todo tráfego é encaminhado para um *gateway*. Devido a estas características, os *gateways* tornam-se os gargalos de uma WMN, afetando drasticamente o cálculo da capacidade.

Entre os trabalhos que abordam o cálculo da capacidade das WMN destacam-se [Jun e Sichitiu 2003] e [Aoun e Boutaba 2006].

[Jun e Sichitiu 2003] resolveram o problema para o cálculo da capacidade das WMN utilizando o conceito de domínio de colisão (ou contenção). Apesar de determinar a capacidade de uma WMN, o trabalho considera somente o domínio de colisão com a maior carga da rede e não leva em conta o reuso espacial dentro dos domínios de colisão, reduzindo a eficiência de utilização dos recursos da rede.

[Aoun e Boutaba 2006] estendem o método proposto por [Jun e Sichitiu 2003] considerando vários domínios de colisão e o reuso espacial, tornando a estimativa da capacidade mais próxima da real.

Baseado nos trabalhos de [Jun e Sichitiu 2003] e [Aoun e Boutaba 2006] é possível identificar um método para o cálculo da capacidade das redes sem fio fundamentado na teoria de grafos, nos domínios de colisão e na capacidade teórica do canal, conforme apresentado por [Jun *et al.* 2003].

Segundo [Pióro e Medhi 2004], para se obter uma solução aproximada e ao mesmo tempo satisfatória para o problema de alocação de recursos e identificação dos melhores caminhos da rede, pode-se utilizar métodos de otimização heurísticos como *Differential Evolution* (DE), *Simulated Annealing* (SA), *Nelder-Mead* (NM) e *Random Search* (RS), pois o excessivo número de variáveis e restrições impostas por grandes redes tornam as abordagens baseadas em *Linear Programming* (LP) inadequadas, uma vez que podem falhar e/ou levar muito tempo para convergir a uma resposta quando aplicadas diretamente.

O objetivo deste trabalho é utilizar os conceitos de domínio de colisão, nós escondidos, reuso espacial, capacidade teórica do canal e dos métodos de otimização heurísticos para propor um método capaz de identificar se uma determinada demanda de tráfego pode ou não ser admitida na rede, propondo os caminhos a serem utilizados e a carga associada a cada caminho. Com o método apresentado é possível realizar engenharia de tráfego em redes *mesh* sem fio baseadas no padrão IEEE 802.11, obtendo o melhor provisionamento possível da rede sem exceder a capacidade dos enlaces sem fio. O método se baseia nas premissas de que todos os nós operam no mesmo canal, considerando uma única interface de rádio por nó da WMN, e que não existe mobilidade nos nós do *backbone*.

As próximas seções do artigo estão organizadas da seguinte forma: a Seção 2 apresenta o Cálculo da Capacidade Teórica do Canal; a Seção 3 descreve os Domínios de Colisão, Reuso Espacial e Nós Escondidos; a Seção 4 apresenta a Proposta para

Engenharia de Tráfego em redes *mesh* sem fio; a Seção 5 apresenta a Análise dos Resultados e a Seção 6 a Conclusão e os Trabalhos Futuros.

2. Capacidade Teórica do Canal

Segundo [Jun *et al.* 2003], a capacidade teórica do canal (*TMT - Theoretical Maximum Throughput*) das redes IEEE 802.11 pode ser obtida através da divisão do número de bits do MSDU (*MAC Service Data Unit*) pelo atraso total para se enviar um MSDU, conforme a Expressão 1, onde Nb_{pkt} representa o tamanho do pacote em bytes, e α e β as componentes de atraso para se enviar um *MSDU*.

$$TMT\left(Nb_{pkt}\right) = \frac{8 \times Nb_{pkt}}{\alpha \times Nb_{pkt} + \beta} \times 10^6 \, bps \qquad (1)$$

Os valores de α e β são definidos conforme o padrão (802.11a, 802.11b, etc), a técnica de codificação e modulação (FHSS, DSSS, OFDM, etc) e a taxa de transmissão (Mbps) utilizada, sendo definidos no trabalho de [Jun *et al.* 2003].

A *TMT* é definida sobre as seguintes suposições: BER (*Bit Error Rate*) igual a zero; não existem perdas devido a colisões; PCF (*Point Coordination Function*) não é utilizado; não ocorrem perdas de pacotes devido a estouro das filas no receptor, a camada MAC não usa fragmentação, e os quadros de gerenciamento não são considerados.

3. Domínios de Colisão, Reuso Espacial e Nós Escondidos

Conforme [Jun e Sichitiu 2003] e [Aoun e Boutaba 2006], o domínio de colisão de um enlace sem fio, composto por um nó transmissor e um nó receptor, é formado pelo conjunto de todos os enlaces vizinhos que compartilham seu canal local, e consequentemente interferem em sua transmissão.

Pode-se dizer que o domínio de colisão de um nó transmissor é formado pelo conjunto de nós receptores cuja distancia seja menor ou igual á distância de interferência e consequentemente à distância de transmissão.

Considerando o exemplo da Figura 1, a distância entre nós de 200 metros, distância de transmissão de 250 metros e a distância de interferência de 550 metros, defini-se o conjunto de domínio de colisão do nó 3, como CDC_{N3}={N_5, N_4, N_3, N_2, N_1}. Da mesma forma é possível definir o domínio de colisão para CDC_{N5}={N_5, N_4, N_3}, e os outros nós da Figura 1.

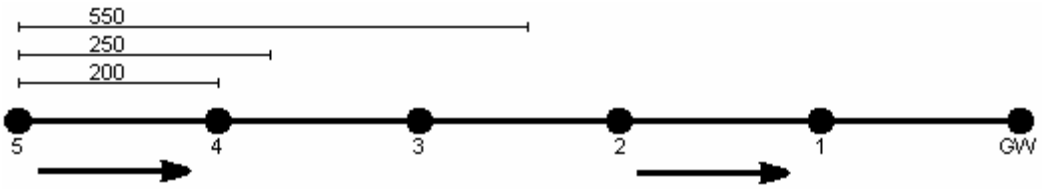


Figura 1. Domínios de Colisão e Reuso Espacial

[Xu *et al.* 2002] demonstraram que o problema do nó escondido ainda pode existir em redes de múltiplos saltos, mesmo com o uso do *four-way handshaking* (RTS - *Request To Send* / CTS - *Clear To Send*) e do CSMA / CA (*Sense Multiple Access with*

Collision Avoidance). Para topologias com mais de quatro saltos, como a da Figura 1, é possível observar o problema do nó escondido nos seguintes pares de nós: $\{N_5, N_2\}$ e $\{N_4, N_1\}$.

Como os nós N_5 e N_2 estão fora do alcance mútuo (distância de interferência), ambos podem acessar o canal, conforme o CSMA / CA, porém isso faz com que o fluxo $N_5 \rightarrow N_4$ não seja atendido, pois N_5 não pode perceber as transmissões de N_2, tentará acessar o canal e N_4 não responderá ao RTS enviado por N_5, devido às transmissões de N_2, fazendo com que o tempo de *backoff* de N_5 aumente exponencialmente. Além disso, caso N_5 consiga realizar a troca do RTS / CTS com sucesso, o fluxo $N_2 \rightarrow N_1$ irá interferir com o fluxo $N_5 \rightarrow N_4$, causando colisões em N_4. Por essas razões, N_2 (que é um nó escondido para N_5) deve pertencer ao domínio de colisão do nó 5, $CDC_{N5}=\{N_5, N_4, N_3, N_2\}$. Uma análise similar é realizada para os nós N_4 e N_1 quando N_4 transmite para N_3, $N_4 \rightarrow N_3$.

Segundo [Aoun e Boutaba 2006], o reuso espacial é identificado quando dois ou mais nós, dentro do mesmo domínio de colisão, podem transmitir simultaneamente sem gerar interferência mútua. Desta forma, para se contabilizar o reuso espacial, realiza-se o complemento (\) do conjunto dos nós da rede, $V=\{N_1, N_2, N_3, N_4, N_5, GW\}$, com o domínio de colisão de cada nó. Considerando o nó N_5, temos $(V \setminus CDC_{N5})=\{N_1, GW\}$, portanto, N_5 pode transmitir simultaneamente com os nós N_1 e GW.

O reuso espacial é computado removendo-se a menor carga do par de enlaces de transmissões simultâneas da carga do domínio de colisão, assim, considerando o domínio de colisão $CDC_{N3}=\{N_5, N_4, N_3, N_2, N_1\}$ como exemplo, verifica-se o reuso espacial de cada nó que pertence ao CDC_{N3}. Conforme descrito no parágrafo anterior, temos que N_5 pode transmitir simultaneamente com N_1, portanto deve-se desconsiderar a transmissão com a menor carga do par $\{N_5, N_1\}$. Desta forma, defini-se a carga do CDC_{N3} como a soma de todas as cargas transmitidas pelos nós: $N_4 + N_3 + N_2 + \text{Min}\,[N_5, N_1]$. A mesma análise deve ser estendida a todos os domínios de colisão.

4. Proposta

O algoritmo proposto neste trabalho utiliza os conceitos de engenharia de tráfego para escolher os caminhos por onde os fluxos (demanda de tráfego) serão transmitidos, dos métodos de otimização heurísticos para busca de um resultado satisfatório para os problemas de alocação dos recursos da rede, e do cálculo da capacidade da rede para evitar que as cargas admitidas na rede excedam a capacidade dos enlaces sem fio.

Dada uma determinada demanda ou um grupo de demandas, com seus endereços de origem e destino (*gateway*), o algoritmo é capaz de identificar se a demanda pode ou não ser admitida na rede, propondo os melhores caminhos e a carga associada a cada caminho, e se for o caso, identificar a porção da demanda que não pode ser atendida.

O algoritmo para realizar engenharia de tráfego às WMN está estruturado em seis etapas principais:

1. Definição dos Parâmetros de Entrada;
2. Construção do Grafo de Conectividade;
3. Identificação dos Caminhos, Domínios de Colisão e Reuso Espacial;

4. Cálculo da Carga das Arestas, Domínios de Colisão e *TMT*;
5. Algoritmo de Otimização
   5.1. Construção da Função Custo;
   5.2. Identificação das Restrições / Variáveis;
   5.3. Execução do Método Heurístico (DE, SA ou NM);
6. Resultados.

As etapas do algoritmo foram formalizadas segundo a notação Z, e são apresentadas nas próximas seções.

4.1. Parâmetros de Entrada

Os parâmetros de entrada definidos para o algoritmo são:

- Identificação do conjunto de vértices (*V*), com a posição dos vértices no plano cartesiano bidimensional, em metros;
- Distância de transmissão (*DT*) e interferência (*DI*), em metros;
- Definição do conjunto de nós ativos (*CNA*) que estão transmitindo em direção ao *gateway* (*GW*), que pode ser diferente para cada nó ativo;
- Identificação do tamanho dos pacotes (bytes), taxa de transmissão (Mbps), esquema de modulação e codificação (FHSS, OFDM, DSSS, HR-DSSS) e o padrão (802.11a, 802.11b, 802.11g, etc) para o cálculo da *TMT*;
- Número máximo de caminhos permitidos por nó ativo (*NMC*), pois o tráfego enviado por um nó ativo pode ser distribuído por um ou mais caminhos simultaneamente, e o número máximo de saltos permitido (*NMS*) por caminho;
- Definição das demandas (*d*) de cada nó ativo.

4.2. Construção do Grafo de Conectividade

O grafo de conectividade *G(V,A)* é representado por um conjunto de vértices *V*, definido nos parâmetros de entrada, e por um conjunto de arestas *A*. As arestas representam a conectividade entre dois vértices do grafo através do padrão IEEE 802.11, e são identificadas pela tupla contendo um vértice transmissor v_i e um vértice receptor v_j.

O conjunto de arestas (*A*) é composto por todos os pares de vértices que apresentam valor da distância euclidiana bidimensional (*DEB*) menor ou igual ao valor da *DT*, conforme definido na Expressão 2.

$$A = \left\{ \forall v_i, v_j \in V \mid \sqrt{\left|\left(x_{v_i} - x_{v_j}\right)\right|^2 + \left|\left(y_{v_i} - y_{v_j}\right)\right|^2} \leq DT \bullet \{v_i, v_j\} \right\} \quad (2)$$

De forma semelhante ao que foi definido para as arestas, o conjunto de vértices na área de interferência (*CVAI*) é definido conforme a Expressão 3.

$$CVAI_{v_i} = \left\{ \forall v_j \in V \mid \sqrt{\left|\left(x_{v_i} - x_{v_j}\right)\right|^2 + \left|\left(y_{v_i} - y_{v_j}\right)\right|^2} \leq DI \bullet v_j \right\} \quad (3)$$

O *CVAI* de um vértice qualquer é composto por todos os vértices que apresentam valor da *DEB* menor ou igual à *DI*, incluindo o próprio vértice em análise e os vértices na *DT*.

4.3. Identificação dos Caminhos, Domínios de Colisão e Reuso Espacial

Os caminhos entre a origem (nós ativos - *CNA*) e o destino (*GW*) são obtidos através do uso de um método de *n* caminhos mais curtos, adaptado do algoritmo de Dijkstra, que após encontrar o caminho mais curto entre a origem e o destino, altera o peso das arestas deste caminho, uma a uma, e procura novos caminhos alternativos. O processo é repetido para todos os nós ativos até que todos os caminhos sejam encontrados. Um caminho é considerado válido somente se o número de saltos for menor do que o *NMS*.

Cada caminho é representado por uma expressão $p_x c_y$ que identifica o próprio caminho (com a sequência de vértices da origem até o destino) e a carga associada a este caminho, atribuída pelos métodos de otimização, onde *x* representa o índice do nó ativo no *CNA* e *y* um dos *n* caminhos encontrados. Os *n* caminhos de cada nó ativo são identificados por K_x.

Conforme definido por [Jun e Sichitiu 2003] e [Aoun e Boutaba 2006], um domínio de colisão representa o conjunto de nós que devem estar inativos para que outro nó possa transmitir com sucesso. Para identificar o conjunto de domínio de colisão (*CDC*) primeiro é necessário identificar o conjunto de arestas na área de transmissão (*CAAT*) de todos os vértices do grafo, conforme a Expressão 4.

$$CAAT_{v_i} = \left\{ \forall a_k \in A \mid v_{i_{a_k}} == v_i \bullet \left\{ v_{i_{a_k}}, v_{j_{a_k}} \right\} \right\} \quad (4)$$

O *CAAT* de um vértice qualquer do grafo é composto por todas as arestas cujo vértice transmissor seja igual ao vértice analisado v_i. Ou seja, o *CAAT* identifica todas as transmissões possíveis de um vértice do grafo. Assim que o *CAAT* foi identificado é possível formar o *CDC*, conforme a Expressão 5.

$$CDC_{a_k} = \left\{ \forall v_i \in \left\{ CVAI_{v_{i_{a_k}}} \bigcup CVAI_{v_{j_{a_k}}} \right\} \mid CAAT_{v_i} \right\} \quad (5)$$

O *CDC* de uma aresta qualquer do grafo é composto pelo *CAAT* de todos os vértices que compõem a união do *CVAI* do vértice transmissor v_i com o *CVAI* do vértice receptor v_j da aresta analisada a_k.

Segundo [Aoun e Boutaba 2006], o reuso espacial é identificado quando dois ou mais vértices, que pertencem ao mesmo domínio de colisão, podem transmitir simultaneamente sem gerar interferência mútua. Para identificar o conjunto de reuso espacial (*CRE*), primeiro é necessário identificar o conjunto de vértices que podem transmitir simultaneamente (*CVTS*), conforme a Expressão 6.

$$CVTS_{a_k} = \left\{ V \setminus \left\{ CVAI_{v_{i_{ak}}} \bigcup CVAI_{v_{j_{ak}}} \right\} \right\} \quad (6)$$

O *CVTS* de uma aresta qualquer é definido através do complemento (\) do conjunto de vértices (*V*), com a união do *CVAI* do vértice transmissor v_i com o *CVAI* do vértice receptor v_j da aresta analisada a_k.

Na sequência, o conjunto de arestas de transmissões simultâneas (*CATS*) de todas as arestas do grafo é definido conforme a Expressão 7.

$$CATS_{a_k} = \left\{ \forall v_i \in CVTS_{a_k} \mid \left(\forall a_i \in CAAT_{v_i} \mid v_{j_{a_i}} \notin \left\{ CVAI_{v_{i_{a_k}}} \bigcup CVAI_{v_{j_{a_k}}} \right\} \right) \bullet a_i \right\} \quad (7)$$

O *CATS* de uma aresta qualquer é formado pelo *CAAT* de todos os vértices do *CVTS*, excluindo-se as arestas cujo vértice receptor pertença à união do *CVAI* do vértice transmissor v_i com o *CVAI* do vértice receptor v_j da aresta analisada a_k.

Assim que o *CATS* foi identificado, é possível formar o *CRE* com o par de arestas de transmissões simultâneas, conforme a Expressão 8.

$$CRE_{a_k} = \left\{ \forall a_i \in CDC_{a_k} \mid \left\{ CATS_{a_i} \bigcap CDC_{a_k} \right\} \neq \{\ \} \bullet \left\{ a_i \times \left\{ CATS_{a_i} \bigcap CDC_{a_k} \right\} \right\} \right\} \quad (8)$$

O *CRE* de uma aresta qualquer é definido através da análise do *CATS* de todas as arestas do *CDC* da aresta analisada a_k. Assim, se existir uma aresta comum ao *CATS* com o *CDC*, tem-se uma transmissão simultânea dentro do mesmo domínio de colisão.

4.4. Cálculo da Carga das Arestas, Domínios de Colisão e *TMT*

A soma das cargas de uma aresta (*SCA*) qualquer do grafo é composta pela soma das cargas de todos os caminhos ($p_x c_y$) que utilizam esta aresta, definida conforme a Expressão 9.

$$SCA_{a_k} = \left(p_{x1} c_{y1} + \ldots + p_{xn} c_{ym} \right) \quad (9)$$

A soma das cargas do domínio de colisão (*SCDC*) é definida conforme a Expressão 10.

$$SCDC_{a_k} = \left(\sum_{\forall a_i \in CDC_{a_k}} SCA_{a_i} \right) - \left(\sum_{\forall a_j \in CRE_{a_k}} - Min\left[SCA_{i_{a_j}}, SCA_{j_{a_j}} \right] \right) \quad (10)$$

A *SCDC* de uma aresta qualquer é formada pela *SCA* de todas as arestas que fazem parte do *CDC* menos o valor da aresta com a menor carga (*Min*) do par de arestas de transmissões simultâneas do reuso espacial da aresta analisada (*CRE*), conforme sugerido por [Aoun e Boutaba 2006].

O cálculo da *TMT* é realizado conforme a Expressão 1, proposta por [Jun *et al.* 2003], com os parâmetros da camada MAC definidos como entrada para o algoritmo.

4.5. Algoritmo de Otimização

Antes de iniciar o processo de otimização é necessário definir a função custo a ser minimizada, as restrições que devem ser respeitadas e as variáveis envolvidas na otimização.

A função custo para minimizar a demanda não atendida (*dna*) de cada demanda (*d*), é definida conforme a Expressão 11.

$$fc_{\min} = dna_1 + \ldots + dna_i + \ldots + dna_I \text{, onde } i \in \left[1, |CNA|\right] \quad (11)$$

A seguintes restrições são definidas para os métodos de otimização:

- Número máximo de caminhos (Expressão 12): limita o número máximo de caminhos permitido por nó ativo. As combinações de caminhos possíveis são obtidas através da permutação (*Perm*) dos *n* caminhos encontrados, contendo exatamente *NMC*. A

restrição também determina que a soma (*Total*) da maior carga (*Max*) dos caminhos mais a demanda não atendida seja exatamente igual à demanda requisitada.

$$dna_i + Max\left[Total\left[Perm\left[\left\{p_1c_1,\ldots,p_ic_n,\ldots,p_Ic_N\right\},NMC\right]\right]\right] == d_i \text{, onde}$$
$$i \in \left[1,\left|CNA\right|\right] \text{ e } n \in \left[1,\left|K_i\right|\right] \quad (12)$$

- Restrição positiva (Expressão 13): garante que o valor das variáveis envolvidas no processo de otimização seja maior ou igual a zero. Evita que sejam atribuídos valores negativos às variáveis durante a otimização.

$$p_1c_1 \geq 0 \ldots p_ic_n \geq 0 \ldots p_Ic_N \geq 0 \ldots dna_1 \geq 0 \ldots dna_i \geq 0 \ldots dna_I \geq 0 \text{, onde}$$
$$i \in \left[1,\left|CNA\right|\right] \text{ e } n \in \left[1,\left|K_i\right|\right] \quad (13)$$

- Número máximo de iterações: atua como critério de parada para o algoritmo. Determina o número máximo de gerações sem melhoria
- Carga máxima do domínio de colisão (Expressão 14): garante que o domínio de colisão com a maior carga da rede (*Max*) não exceda o valor da *TMT*.

$$Max\left\lfloor SCDC_{a_1},\ldots,SCDC_{a_i},\ldots,SCDC_{a_I}\right\rfloor \leq TMT \text{ , } \forall a_i \in A \quad (14)$$

A lista com as variáveis utilizadas durante a otimização é definida conforme a Expressão 15, onde as cargas dos caminhos, atribuídas pelos métodos de otimização, são limitadas ao valor da *TMT* para restringir o universo de valores possíveis.

$$\left\{\left\{p_1c_1,0,TMT\right\},\ldots,\left\{p_ic_n,0,TMT\right\},\ldots,\left\{p_Ic_N,0,TMT\right\},\ldots dna_1 \ldots dna_i \ldots dna_I\right\},$$
$$\text{onde } i \in \left[1,\left|CNA\right|\right] \text{ e } n \in \left[1,\left|K_i\right|\right] \quad (15)$$

4.7. Resultados

Como resultado da execução do algoritmo proposto temos uma lista de caminhos, limitada por NMC e NMS, para cada nó ativo (*CNA*) até o respectivo destino (*GW*) e a identificação da carga máxima que pode ser admitida em cada caminho sem que a capacidade da rede seja excedida. Os resultados podem ser classificados da seguinte forma:

- Demanda não atendida diferente de zero. Significa que as demandas solicitadas podem ser parcialmente admitidas na rede;
- Demanda não atendida igual a zero. Significa que todas as demandas solicitadas podem ser admitidas na rede com a carga solicitada;

5. Análise dos Resultados

Os resultados obtidos pelo algoritmo proposto, denominado Atender Demanda - AD, foram comparados com os resultados dos métodos propostos por [Jun e Sichitiu 2003] (*Nominal Capacity* - NC) e [Aoun e Boutaba 2006] (*Max Min Fair Capacity* - MMFC).

Para a análise dos resultados apresentados neste artigo considerou-se uma WMN com 18 nós, *DT* = 250 metros e *DI* = 550 metros, onde todos os nós operam no padrão

IEEE 802.11b com RTS/CTS, taxa de transmissão de 11 Mbps e usam o HR-DSSS como técnica de codificação e modulação, resultando na *TMT* = 4.515 Kbps.

Inicialmente considerou-se somente um nó ativo (nó 2), transmitindo em direção ao *gateway* (nó 10), cuja demanda (*d*) solicitada é de 2.576 Kbps, conforme demonstra a Figura 2.

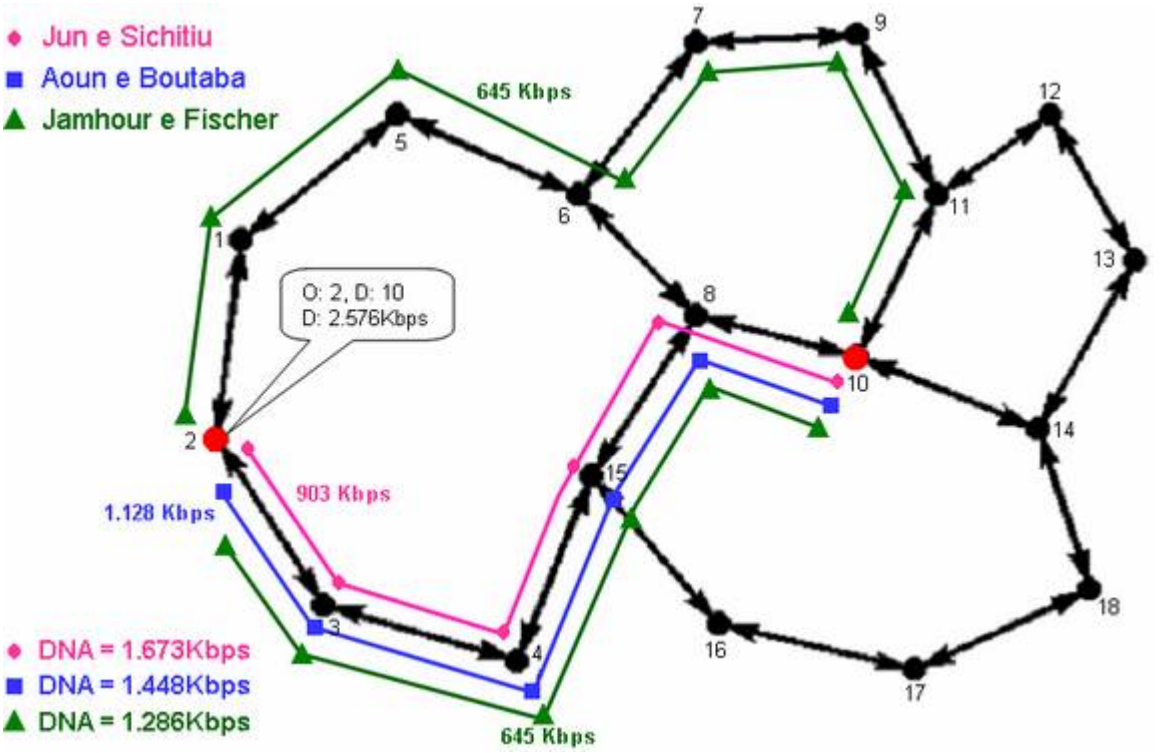


Figura 2. Análise dos Resultados para 1 Nó Ativo

Analisando a Figura 2 é possível verificar que o método NC foi capaz de admitir 903 Kbps, resultando na demanda não atendida de 1.673 Kbps, enquanto o método MMFC foi capaz de admitir 1.128 Kbps, resultando na demanda não atendida de 1.448 Kbps, utilizando o mesmo caminho proposto por NC. Esta diferença entre os dois métodos é atribuída ao uso do reuso espacial pelo método MMFC.

Considerando o método AD, percebe-se que o tráfego gerado pelo nó ativo 2 foi distribuído por dois caminhos distintos, propostos pelos métodos de otimização, cujas cargas admitidas foram de 645 Kbps para cada caminho, resultando na demanda não atendida de 1.286 Kbps.

É importante observar que os métodos NC e MMFC não são capazes de distribuir a demanda de um nó por múltiplos caminhos uma vez que o número de variáveis resultante desta abordagem não é tratável analiticamente.

O gráfico da Figura 3 apresenta a soma das demandas não atendidas, considerando 1 nó ativo com 1, 2, 3 e 4 caminhos e os métodos NC, MMFC e AD. É possível verificar que conforme o número de caminhos disponíveis por nó ativo aumenta, mais carga pode ser admitida na rede com o uso do método AD, estabilizando em 2 caminhos por nó ativo. O que pode ser justificado porque os nós que compõem os

caminhos alternativos pertencem aos mesmos domínios de colisão, limitando o uso de mais de dois caminhos para a topologia da Figura 2.

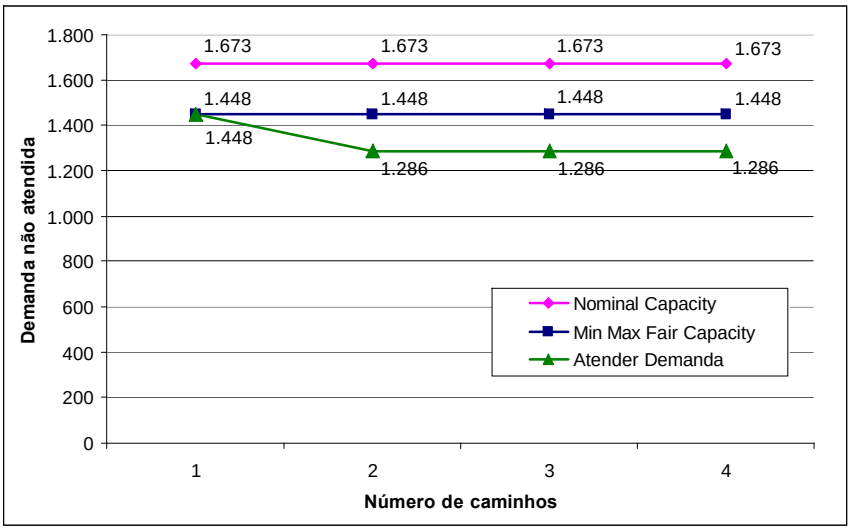


Figura 3. Demanda não atendida x Método de Otimização – 1 Nó Ativo

Analisando a Figura 4, com dois nós ativos (nó 2 e nó 15) transmitindo em direção ao *gateway* (nó 10), com demanda (*d*) solicitada de 2.576 Kbps para cada nó ativo, é possível verificar que os resultados obtidos pelo algoritmo proposto são mais expressivos.

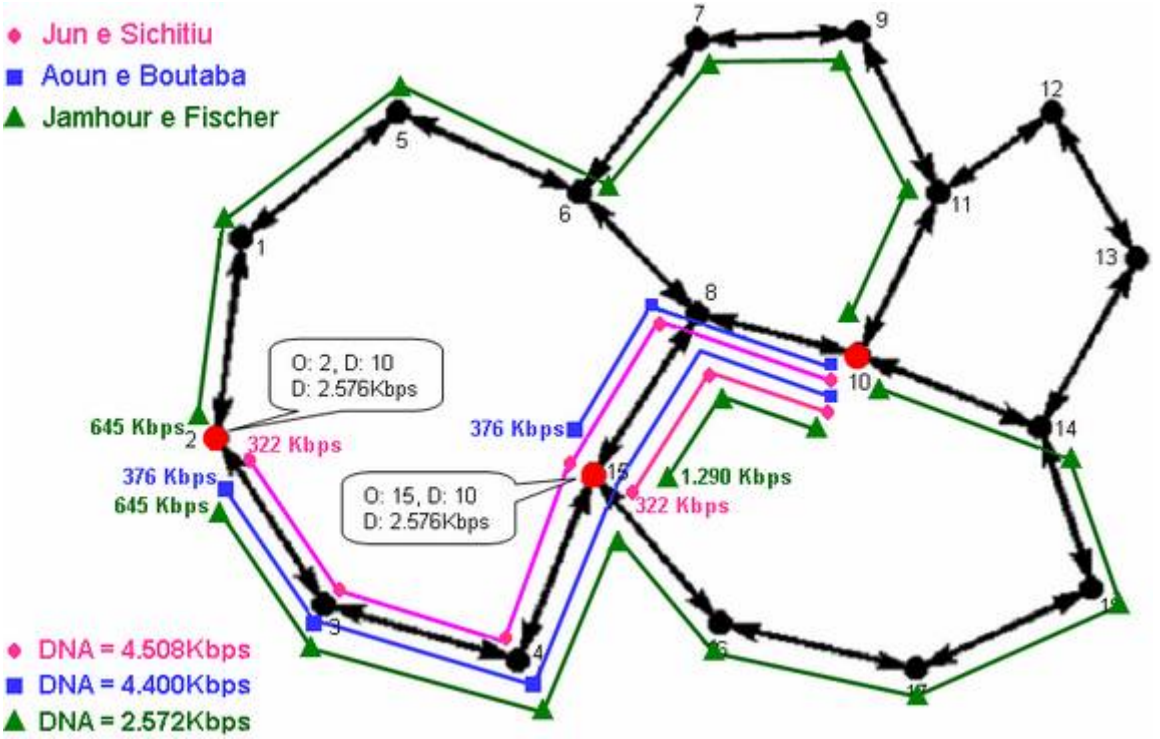


Figura 4. Análise dos Resultados para 2 Nós Ativos

Considerando o método NC, foi possível admitir 322 Kbps em cada caminho, resultando na demanda não atendida total de 4.508 Kbps. Utilizando o método MMFC

foi possível admitir 376 Kbps em cada demanda, resultando na demanda não atendida total igual a 4.400 Kbps.

Analisando os resultados do método AD, percebe-se que as demandas dos dois nós ativos foram distribuídas por três caminhos distintos, onde foi possível admitir 1.290 Kbps para atender a demanda do nó 15, e 645 Kbps em cada um dos caminhos propostos para a demanda do nó 2, resultando na demanda não atendida total de 2.572 Kbps.

O gráfico da Figura 5 apresenta a soma das demandas não atendidas, considerando 2 nós ativos com 1, 2, 3 e 4 caminhos e os métodos NC, MMFC e AD. É possível verificar que conforme o número de nós ativos aumenta, os métodos NC e MMFC não são capazes de distribuir as demandas de tráfego por outros caminhos pois utilizam sempre a estratégia do caminho mais curto, independente da carga das arestas (enlaces). Utilizando o método proposto (AD) foi possível distribuir o tráfego das duas demandas por diferentes caminhos, resultando na melhora do uso dos recursos da rede.

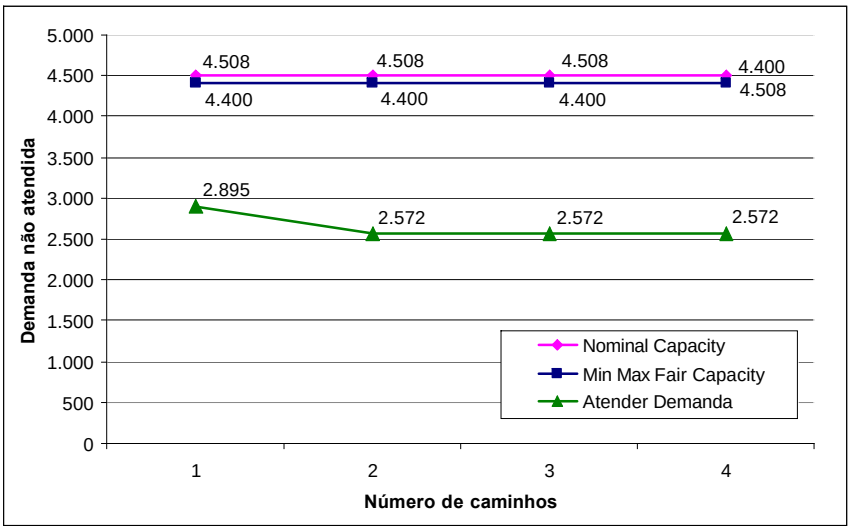


Figura 5. Demanda não atendida x Método de Otimização – 2 Nós Ativos

A Figura 6 apresenta o tempo médio de convergência dos métodos de otimização heurísticos DE, SA e NM, utilizados com o método AD, para 2 (nó 2 e nó 15) e 3 (nó 2, nó 15 e nó 17) nós ativos com 1, 2, 3 e 4 caminhos por nó ativo. Analisando a Figura 6 é possível perceber que o número de caminhos por nó ativo não influencia no tempo total de convergência do algoritmo, o que não ocorre com a adição de mais nós ativos.

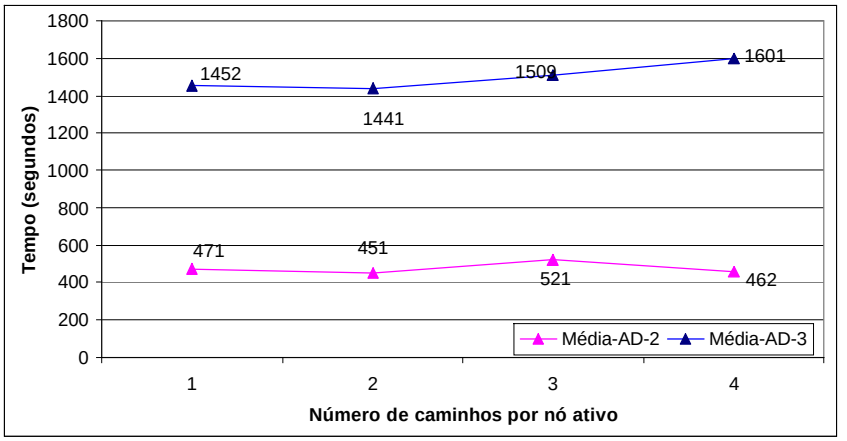


Figura 6. Média dos Tempos de Convergência

Analisando a Figura 7, onde foram considerados dois caminhos por nó ativo e o algoritmo de otimização DE no método AD, é possível verificar que o tempo de convergência é diretamente influenciado pelo número de nós ativos inseridos na simulação, pois cada nó ativo acrescenta uma quantidade considerável de variáveis ao problema de otimização.

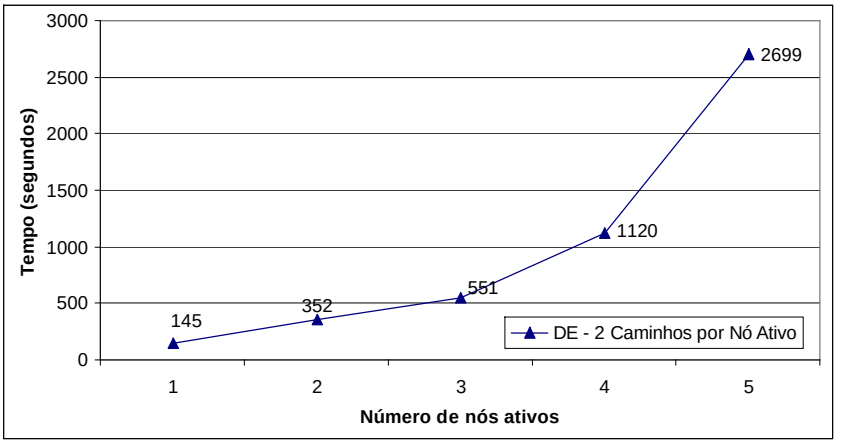


Figura 7. Tempo de Convergência x Número de Nós Ativos

6. Conclusão e Trabalhos Futuros

Este estudo apresentou um método para maximizar o uso dos recursos de uma rede *mesh* sem fio de um único canal, baseada no padrão IEEE 802.11. O algoritmo proposto emprega os conceitos de domínio de colisão, reuso espacial e nós escondidos para identificação da carga da rede, e de métodos de otimização baseados em heurísticas para resolver o problema de alocação dos recursos da rede.

Demonstramos através de simulações e comparações que o método é capaz de realizar engenharia de tráfego para as WMN respeitando a capacidade máxima do canal, informando ao final da otimização se a demanda solicitada pode ou não ser admitida na rede, os caminhos que devem ser utilizados e da carga máxima permitida em cada caminho.

Entre as topologias analisadas, podemos concluir que conforme o número de caminhos alternativos entre a origem e o destino aumenta, os resultados do algoritmo proposto também melhoram quando comparados aos métodos NC e MMFC, que não são capazes de distribuir a demanda de um nó por múltiplos caminhos, uma vez que o número de variáveis resultantes dessa abordagem não é tratável analiticamente. Também foi possível constatar que para redes menores, com número reduzido de caminhos alternativos, não há melhora no uso dos recursos da rede, assim como, quando a origem e o destino estão muito próximos, pois isso faz com que a maioria dos nós responsáveis pelo encaminhamento do tráfego pertença aos mesmos domínios de colisão, limitando a capacidade da rede.

Como trabalhos futuros, pretendemos estender o método proposto adicionando suporte à tolerância a falhas através da identificação dos caminhos principais, por onde os fluxos agregados devem seguir, e dos caminhos de recuperação que devem ser utilizados em caso de falhas. A adição de mais interfaces de rádio (canais) nos nós do domínio de colisão com a maior carga da rede também pode ser considerada, conforme proposto por [Aoun et al. 2006].

Diferentes esquemas de modulação e codificação (MCS - *Modulation and Coding Schemes*), relação sinal ruído (SINR - *Signal to Interference plus Noise Ratio*) e força do sinal recebido (RSS - *Received Signal Strength*) também podem ser considerados, conforme apresentado por [Max *et al.* 2007], porém isso implica em considerável aumento de complexidade ao algoritmo de otimização devendo ser feito um estudo com novas abordagens.

Referências

P. Gupta e PR Kumar, “The Capacity of Wireless Networks” IEEE Transactions on Information Theory’ 2000.

K. Jain, J Padhye, V. Padmanabhan, e L Qiu, “Impact of Interference on Multi-Hop Wireless Network Performance” MobiCom, 2003.

J. Li, C. Blake, D. De Couto, HI Lee e R. Morris, “Capacity of Ad Hoc Wireless Networks” ACM MobiCom, 2001.

J. Jun e ML Sichitiu, “The Nominal Capacity of Wireless Mesh Networks” IEEE Wireless Communications 2003.

J. Jun, P. Peddabachagari, e M. L. Sichitiu, “Theoretical maximum throughput of IEEE 802.11 and its applications” in Proc. Second IEEE International Symposium on Network Computing and Applications (NCA 2003), (Cambridge, MA), pp. 249–256, Abril 2003.

B. Aoun e R. Boutaba, “Max-Min Fair Capacity of Wireless Mesh Networks” IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS). Junho 2006.

K Xu, M Gerla and S Bae, “How Effective is the IEEE 802.11 RTS/CTS Handshake in ad Hoc Networks?”. IEEE Globecom 2002.

M. Pióro e D. Medhi “Routing, Flow, and Capacity Design in Communication and Computer Networks”. Elsevier - 2004.

S. Max, E. Weiss e G. R. Hiertz, “Benefits and Limitations of Spatial reuse in Wireless mesh Networks” Chai of. Communication Networks (ComNets), ACM Outubro 2007.

B. Aoun, R. Boutaba e G. Kenward, “Analysis of Capacity Improvements in Multi-Radio Wireless Mesh Networks”. IEEE Vehicular Technology Conference (VTC), Maio 2006.

Projeto de Topologia Virtual em Redes Ópticas: Uma Abordagem para Evitar a Interferência entre Canais

K. D.R. Assis[1], M. S. Savasini[2], A.F. Santos[3], W. F. Giozza[4]

[1]Universidade Federal da Bahia (UFBA)
CEP: 44210-630 – Salvador – BA – Brasil.

[2]Universidade Estadual de Campinas (UNICAMP)
CEP: 13083-970 – Campinas – SP – Brasil.

[3]Universidade de São Paulo (USP)
CEP: 13566-590 – São Carlos – SP, Brasil.

[4]Universidade de Brasília (UnB)
CEP: 70910-900 – Brasília – DF, Brasil.

karcius.assis@ufba.br,savasini@decom.fee.unicamp.br,afsantos@usp.br e giozza@ene.unb.br

Abstract. *In this paper we propose an strategy to limit the adjacent channels interference in the design of virtual topology of optical networks. The proposed formulation is linear and can provide optimal solutions. In traditional planning strategies of the virtual topology, there is no a priori knowledge of channel usage, and since the solution is implemented, the interference can not be avoided. Taking into account the effects of adjacent channels interference, we extend the traditional formulation with a set of analytical formulas and additional constraints that will limit the interference. A heuristic is also proposed to solve problems with many instances.*

Resumo. *Neste artigo propomos uma estratégia para limitar a interferência de canais adjacentes no projeto de topologia virtual de redes ópticas. A formulação proposta é linear e capaz de fornecer soluções ótimas. Nas estratégias tradicionais de planejamento da topologia virtual, não há nenhum conhecimento a priori do uso do canal, e uma vez que a solução é implementada, a interferência não pode ser evitada. Levando em consideração os efeitos da interferência de canais adjacentes, estendemos a formulação tradicional com um conjunto de fórmulas analíticas como restrições adicionais que permitem limitar a interferência. Uma heurística também é proposta para solucionar problemas com muitas instâncias.*

1. Introdução

Atualmente o número de usuários da Internet vem crescendo exponencialmente. Isto é devido, em parte, ao surgimento de novas aplicações, assim como vídeo sob demanda, teleconferências, imagens médicas de alta resolução etc. Desta forma, tem sido estimulada a pesquisa e o desenvolvimento de novas gerações de redes de transporte, capazes de suportar esses novos tipos de fluxos de informação. Neste contexto, surge um modelo baseado em uma infra-estrutura óptica inteligente, que utiliza a tecnologia

de Multiplexação por Divisão de Comprimento de Onda (WDM – *Wavelength Division Multiplexing*) [Ramaswami, 2006].

A tecnologia WDM proporciona um melhor aproveitamento da capacidade de transmissão das fibras ópticas, possibilitando a transmissão de diversos comprimentos de onda, de forma simultânea, em uma mesma fibra óptica. Desta maneira, com o uso da tecnologia WDM, é possível atender uma maior demanda de tráfego.

Para o estabelecimento de uma conexão, entre dois nós de uma rede óptica WDM transparente (i.e., sem conversão eletro-óptica em nós intermediários), faz-se necessário configurar os caminhos ópticos por onde o tráfego será encaminhado, alocando os recursos indispensáveis para o estabelecimento desta conexão.

Ao se projetar uma rede WDM transparente, deve-se pensar em soluções (caminhos ópticos) que atendam toda a demanda de tráfego da rede, minimizando o custo ou a utilização de seus recursos (quantidade de comprimentos de onda, portas etc) para preservar capacidade aberta ou recursos para demandas futuras, imprevistas, ou para necessidade de reconfigurações, em caso de falha na rede [Banerjee *et al*, 1996], [Assis *et al*, 2009]. A determinação dos caminhos ópticos, baseada na demanda de tráfego é conhecida como Projeto da Topologia Virtual (VTD – *Virtual Topology Design*) e o roteamento na topologia física e alocação de comprimentos de onda para os caminhos ópticos estabelecidos previamente é conhecido como Projeto da Topologia Física (PTD – *Physical Topology Design*) ou Roteamento e Alocação de Comprimentos de Onda (RWA– *Routing and Wavelength Assignment*) [Ramaswami e Sivarajan, 1996], [Assis *et al*, 2005].

Diversos trabalhos apresentados na literatura já abordaram o VTD em redes ópticas, isoladamente ou em conjunto com o RWA. Várias formulações matemáticas e métodos heurísticos sob diferentes hipóteses e padrões de tráfego foram propostos. Veja os estudos realizados por [Dutta e Rouskas, 2000] e [Zang *et al*, 2000] como exemplos de tutoriais que trataram do tema até o ano 2000 e [Pavon-Marino *et al*, 2009], [Jaumard, B. *et al*, 2009] como exemplos de trabalhos mais recentes. Os objetivos de projeto mais freqüentemente estudados são: no caso do VTD, a minimização do congestionamento e a minimização do processamento eletrônico; em relação ao RWA, a minimização do número de comprimentos de onda (chamado de min-RWA) e a maximização do número de conexões que podem ser estabelecidas (chamado de max-RWA).

No entanto, nas redes WDM transparentes, a qualidade do sinal pode ser degradada devido a restrições na camada física. Por exemplo, a interferência entre canais (*crosstalk*) depende da utilização ou não de canais adjacentes ao longo do caminho óptico [Deng *et al*, 2004]. Além disso, os efeitos de outras degradações, como a Modulação Cruzada de Fase (XPM- C*ross Phase Modulation*) e a Mistura de Quatro Ondas (FWM- *Four Wave Mixing*) são altamente dependentes do uso de canais adjacentes ou próximos aos adjacentes, [Azodolmolky, 2009]. Portanto, evitar as interferências entre canais adjacentes é um critério importante para planejar de forma eficiente redes WDM transparentes.

Em [Deng *et al*, 2004] é apresentado um algoritmo de limitação de interferência para o RWA dinâmico e em [Manousakis *et al*, 2008] outro algoritmo de limitação de interferência é apresentado para o RWA estático. O primeiro algoritmo baseia-se na enumeração de interferências introduzidas pela fonte ao longo de um caminho óptico,

considerando que a topologia virtual (caminhos ópticos estabelecidos) é conhecida. O segundo algoritmo está baseado numa formulação através de programação linear sujeita a uma demanda de tráfego estático. Outras abordagens, como a de [He, *et al* 2007], tentam evitar a mistura de quatro ondas e a modulação cruzada de fase.

Diante disso, a solução do RWA tem uma influência importante no surgimento desses efeitos, pois selecionar um caminho óptico, entre um par origem-destino, e alocar um ou vários comprimentos de onda disponíveis nesse caminho pode diminuir ou aumentar as degradações dos efeitos da camada física. Então, o planejamento de redes ópticas transparentes deve ser capaz de considerar em suas decisões os efeitos e propriedades da camada física [Ramamurthy *et al*, 1999]. Nesse caso, as formulações matemáticas e algoritmos são conhecidos como IRWA ou ICBR (*Impairment Constraint Based Routing*) [Bastos Filho *et al*, 2009]. Neste trabalho, propomos uma nova formulação matemática para evitar a interferência entre canais WDM, considerando os enlaces de fibra óptica.

A primeira formulação linear de uma solução parcial do problema RWA, evitando o uso de canais adjacentes, foi proposta em [Manousakis *et al* 2008], onde as restrições são criadas usando uma *path-formulation* [Jaumard *et al*, 2007], em que apenas *K* rotas, das possíveis, são disponíveis para o RWA. Neste trabalho, nossas principais contribuições são:

1) Uma *link-formulation* [Jaumard *et al*, 2007], que é uma extensão do trabalho proposto em [Manousakis *et al* 2008]. Enquanto em [Manousakis *et al* 2008] se conhece previamente o conjunto de *K* rotas alternativas para qual uma conexão pode ser estabelecida; neste trabalho, não conhecemos com antecedência as rotas. Então todas são possíveis. Logo, a formulação linear que propomos pode encontrar resultados eficientes para evitar a interferência entre canais, já que qualquer rota pode ser escolhida e não apenas as pré-estabelecidas.
2) Nossa formulação é um projeto completo de rede, ou seja, a topologia virtual e física são tratadas simultaneamente e comparadas com os resultados de [Krishnaswamy and Sivarajan, 2001], [Ramaswami and Sivarajan, 1996] que não levam em conta os efeitos da interferência entre canais. Dessa forma, observamos o efeito das restrições da camada física em um nível mais alto, ou seja, na configuração da topologia virtual.

Apesar de existirem diversos outros efeitos físicos que afetam o planejamento de redes ópticas transparentes, eles não foram considerados no escopo deste trabalho.

Este artigo está organizado da seguinte forma. Na seção 2 definimos mais detalhadamente topologia virtual e topologia física. Na seção 3 apresentamos a formulação matemática tradicional para solucionar o projeto completo de uma rede óptica (VTD e RWA). Na seção 4 introduzimos detalhadamente o conceito de interferência entre canais adjacentes e acrescentamos as restrições da camada física na formulação da seção 3. Na seção 5 mostramos resultados numéricos para uma topologia de rede com 6 nós, abordamos sobre complexidade computacional e propomos uma heurística para redes de maiores dimensões. Aplicamos a heurística para uma topologia de rede com 14 nós (e.g., NSFNET) e comparamos com os resultados de [Ramaswami e Sivarajan, 1996]. Finalmente, concluímos nosso artigo na seção 6.

2. Topologia Física e Topologia Virtual

Ao projetar uma rede óptica WDM é necessário estabelecer os caminhos ópticos por onde o tráfego (geralmente medido em Gbps) será encaminhado. Essa definição é feita

através do VTD. Posteriormente, o RWA deve ser resolvido, ou seja, os caminhos ópticos, previamente escolhidos, devem ser roteados por uma topologia física e comprimentos de onda devem ser alocados de forma adequada nesses caminhos ópticos. Esse segundo processo deve obedecer às seguintes regras:

a) dois caminhos ópticos podem compartilhar um mesmo enlace, porém, não podem ser associados ao mesmo comprimento de onda em um mesmo enlace físico.

b) se conversões de comprimento de onda não forem permitidas, o caminho óptico deve ser associado ao mesmo comprimento de onda em todos os enlaces da rota.

Essas duas regras se aplicam a este trabalho. A Figura 1 ilustra uma arquitetura de uma rede óptica simples, formando uma topologia física, com os nós numerados de 1 a 6 e interconectados através de enlaces físicos (fibras ópticas) bidirecionais.

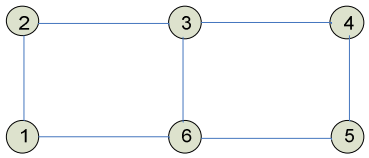


Figura 1. Topologia física

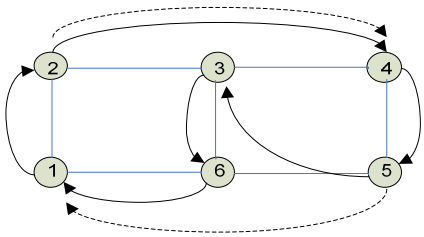


Figura 2. Topologia virtual

O projeto de topologia virtual envolve a definição dos caminhos virtuais para o encaminhamento dos dados entre um par de nós (fonte e destino). Todos os nós da rede se comunicam através dos caminhos virtuais. Se na topologia virtual um nó não estiver conectado diretamente (conectado virtualmente) com o nó destino, então os dados serão conduzidos por várias rotas virtuais até chegarem ao seu destino. Pode-se visualizar isto na Figura 2, onde, o nó 3 não tem uma conexão direta (caminho virtual) para o nó 1. Então o tráfego originado em 3 terá que passar por dois caminhos virtuais: de 3 para 6 e de 6 para 1 para chegar ao seu destino, o nó 1. A quantidade de caminhos ópticos utilizados, também é chamada de saltos virtuais (*virtual hops*). No exemplo anterior, houve a utilização de dois caminhos ópticos, então se diz que ocorreram dois saltos virtuais. Coincidentemente, também ocorreu a passagem por dois enlaces físicos. Neste exemplo, limitamos para 2 o número de enlaces físicos que um caminho óptico pode percorrer. O número máximo de enlaces físicos que um caminho óptico pode percorrer é denotado por H e o número de comprimentos de onda disponíveis para planejar a rede é denotado por W.

Após o estabelecimento dos caminhos virtuais o RWA deve ser resolvido, obedecendo as regras “a” e “b” estabelecidas anteriormente. Para a topologia virtual da Figura 2, o RWA é mostrado na Tabela 1 abaixo para três diferentes alocações de comprimento de onda. Nota-se que na Solução #1 foi necessário o uso de 2 comprimentos de onda para resolver o RWA. Nessa solução, o segundo comprimento de onda foi necessário no segundo caminho óptico 2-4 e também no caminho óptico direto 5-1 (setas tracejadas na Figura 2). As soluções #2 e #3 serão explanadas na seção 4.

Tabela 1. Possível RWA para a topologia virtual da Figura 2, *W*=3, *H*=2

CAMINHO VIRTUAL	ROTA FÍSICA	SOLUÇÃO #1 COMPRIM. DE ONDA	SOLUÇÃO #2 COMPRIM. DE ONDA	SOLUÇÃO #3 COMPRIM. DE ONDA
1-2	1-2	1	1	1
$(2\text{-}4)^1$	2-3-4	1	1	1
$(2\text{-}4)^2$	2-3-4	2	2	3
3-6	3-6-1	1	1	1
4-5	4-5	1	1	1
5-3	5-6-3	1	1	1
5-1	5-6-1	2	3	3
6-1	6-1	1	1	1

Note que configuramos 8 caminhos ópticos no exemplo acima. Para uma rede com N nós, o ideal seria configurar caminhos ópticos para todos os $N(N-1)$ pares. Entretanto, isso não é usualmente possível por duas razões: Primeiro, o número de comprimentos de onda disponíveis impõe um limite na quantidade de caminhos ópticos que podem ser configurados (isto é também uma função da distribuição de tráfego). Segundo, cada nó pode ser fonte e destino de um número limitado de caminhos ópticos. Isto é determinado pela quantidade de hardware óptico que pode ser provido (transmissores e receptores) e pela quantidade total de informações que um nó pode processar. Daí a importância do VTD, pois o mesmo tenta projetar a rede de forma eficiente para um número limitado de caminhos virtuais, definido por um parâmetro chamado grau virtual.

Então, sendo $T = (\lambda^{sd})$ uma matriz de tráfego, i.e., λ^{sd} é a taxa de pacotes (ou Gbps) de um nó s que são enviados para o nó d. Nós tentamos criar uma topologia virtual G_v e rotear o tráfego nesta G_v minimizando $\lambda_{max} = \max_{ij}\lambda_{ij}$ onde λ_{ij} é a carga oferecida ao enlace (i,j) da topologia virtual. A variável λ_{max} é a máxima carga que atravessa um enlace virtual e é definida como *congestionamento*. Sendo G_p a topologia física da rede, Δ o grau da topologia virtual (grau virtual) e W o número de comprimentos de ondas disponíveis. Uma descrição informal do problema de projeto integrado das topologias virtual, conhecido como VTD, e física, conhecido como PTD, é dada a seguir (uma formulação precisa usando Programação Linear Inteira Mista – MILP– pode ser encontrada em [Ramaswami, R. and Sivarajan, K.N., 1996].

$$\text{Min } \lambda_{max} \quad (1)$$

sujeito a:

- cada enlace virtual em G_v corresponde a um caminho óptico e dois caminhos ópticos que compartilham um arco na topologia física devem ter comprimentos de ondas diferentes;
- o número total de comprimentos de onda usados é no máximo W;
- todos os nós em G_v têm Δ arcos de entrada e Δ arcos de saída;
- o fluxo de tráfego de cada par fonte-destino é conservado nos nós intermediários.

3. Formulação Matemática:

Na formulação apresentada em [Ramaswami, R. e Sivarajan, K.N., 1996], para o VTD, nós adicionamos as restrições do PTD, criando uma formulação matemática mais robusta, fazendo dessa forma a integração dos subproblemas VTD e PTD.

A) Notação:

- *i* e *j* são os nós de origem e término, respectivamente, de um caminho óptico.
- *m* e *n* denotam enlaces físicos de *m* para *n*, nos quais podem passar um ou mais caminhos ópticos.

B) Dado:

- Número de nós na rede: *N*.
- Número de comprimentos de onda disponíveis: *W*
- Topologia física (P_{mn}): denota o número de fibras interconectando os nós *m* e *n*. $P_{mn} = 0$ para um nó *m* que não é fisicamente adjacente a um nó *n*. $P_{mn} = P_{nm}$ indica que deve haver igual número de fibras do nó *m* para *n* e de *n* para *m*. Pode haver mais do que um enlace de fibra conectando nós adjacentes na rede. Entretanto, neste trabalho, por simplicidade, consideramos P_{mn}=P_{nm} = 1.

C) Variáveis:

- Topologia Virtual: a variável inteira $b_{ij} \in \{0,1\}$ denota se existe um caminho óptico de um nó *i* para um nó *j* na topologia virtual. Note que nesta formulação os caminhos ópticos não são necessariamente bidirecionais, isto é, $b_{ij} = 0$ não implica em $b_{ji} = 0$.
- Carga em um enlace físico: *L*, sendo $L \leq W$. A carga denota o número máximo de caminhos ópticos que devem atravessar um enlace físico da rede.
- Roteamento na topologia física: A variável p_{mn}^{ij} denota o caminho óptico entre os nós *i* e *j* que está sendo roteado pelo enlace de fibra *m*-*n*.
- Alocação de comprimento de onda: A variável $p_{mn\varsigma}^{ij}$ especifica o comprimento de onda ς que é alocado ao caminho óptico entre os nós *m* e *n* da topologia física. Como não há conversão de comprimento de onda, esse mesmo valor será alocado para todos os enlaces físicos onde o caminho óptico *i*-*j* passa.

Logo, a formulação matemática através de Programação Linear Inteira Mista (MILP) para os problemas VTD e PTD, de forma integrada, utilizando como função objetivo a equação (1) é dada como a seguir.

- Adicionamos as seguintes restrições PTD ao VTD de [Ramaswami, R. and Sivarajan, K.N., 1996]:

D) PTD- Physical Topology Design

- Roteamento na topologia física p_{mn}^{ij}:

$$\sum_m p_{mk}^{ij} = \sum_n p_{kn}^{ij}, ...se....k \neq i, j \quad (2)$$

$$\sum_n p_{in}^{ij} = b_{ij} \quad (3)$$

$$\sum_m p_{mj}^{ij} = b_{ij} \quad (4)$$

$$\sum_{ij} p_{mn}^{ij} \leq L.P_{mn} \quad (5)$$

As equações (2)-(4) garantem o roteamento dos caminhos ópticos (b_{ij}) na topologia física através de equações de fluxo *multicommodity* . Note que o *commodity* agora é um caminho óptico e não dados como no VTD de [Ramaswami, R. e Sivarajan, K.N., 1996]. A equação (5) limita o número máximo de caminhos ópticos que atravessam um enlace físico através da variável carga *L*. Neste trabalho assumimos que a carga é limitada pelo número de comprimentos de ondas disponíveis *W*.

- Alocação de comprimento de onda e restrições de continuidade de comprimento de onda (sem conversão em nenhum nó)

$$\sum_m p_{ml\varsigma}^{ij} = \sum_n p_{ln\varsigma}^{ij} \qquad se\ l \neq i,j \tag{6}$$

$$\sum_n p_{in\varsigma}^{ij} = b_{ij\varsigma} \tag{7}$$

$$\sum_m p_{mj\varsigma}^{ij} = b_{ij\varsigma} \tag{8}$$

$$\sum_\varsigma b_{ij\varsigma} = b_{ij} \tag{9}$$

$$\sum_{ij} p_{mn\varsigma}^{ij} \leq P_{mn} \tag{10}$$

$$\sum_\varsigma p_{mn\varsigma}^{ij} = p_{mn}^{ij} \tag{11}$$

As equações (6)-(11) permitem a alocação adequada de comprimentos de onda para os caminhos ópticos roteados na topologia física. Note que as restrições não permitem conversão de comprimento de onda nos nós intermediários da rede.

- Condição de não-negatividade e número inteiros

int p_{mn}^{ij}, $p_{mn\varsigma}^{ij}$ e $p_{mn}^{ij} \geq 0, p_{mn\varsigma}^{ij} \geq 0$

4. Interferência entre Canais no RWA

Como mencionado anteriormente, nas redes WDM transparentes, a qualidade do sinal é degradada devido às restrições da camada física. Essas restrições dependem das características físicas das fibras usadas, mas algumas dessas restrições também variam de acordo com a utilização da rede. Por exemplo, a interferência entre canais, a modulação cruzada de fase (XPM) e a mistura de quatro ondas (FWM) não dependem unicamente das características da fibra, mas também da utilização de outros comprimentos de onda no mesmo enlace. Portanto, neste caso, temos que levar em consideração como a alocação de comprimentos de onda irá interferir na solução do RWA. Uma proposta é apresentada na próxima subseção.

4.1 Adjacência entre Canais

Nesta subseção, iremos melhorar a formulação apresentada na seção 3 para levar em consideração a interferência entre canais adjacentes na mesma fibra. Para tanto, definiremos interferência entre canais e descreveremos o efeito da interferência do canal adjacente com uma fórmula analítica, aplicada aos enlaces que compõem o caminho. Posteriormente, restringiremos a interferência total de canais adjacentes sobre um enlace, de modo a ser inferior a um limite pré-definido. As definições a seguir, juntamente com a Figura 3, são necessárias para uma melhor compreensão deste trabalho.

A) Definições:

- Distância entre dois comprimentos de onda:

  -a distância entre dois comprimentos de onda, a e b, é dada por:

$$d(\varsigma_a, \varsigma_b) = | \varsigma_a - \varsigma_b |$$

- Comprimentos de onda adjacentes:

  -dois comprimentos de onda são chamados adjacentes se a distância entre eles é:

$$d(\varsigma_a, \varsigma_b) = 1$$

- Interferência de dois comprimentos de onda no mesmo enlace:

  -dois comprimentos de onda interferem entre si quando são adjacentes. Isto acontece se a distância entre eles é 1.

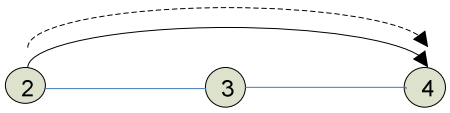


Figura 3. Configuração parcial da rede da Figura 1. Exemplo de interferência, se ς_a=1e ς_b=2 d(ς_a, ς_b) = | 1 - 2 | =1

Retornando à solução #1 da seção 2 observamos que os caminhos ópticos 2-4 interferem um com o outro (nos enlaces 2-3 e 3-4), pois possuem alocações de comprimentos de onda adjacentes d(1,2) = | 1 - 2 | =1. O mesmo ocorre com os caminhos ópticos 6-1 e 5-1, pois também possuem alocações de comprimentos de onda adjacentes, ocorrendo a interferência no enlace físico 6-1. Logo, há 3 interferências na solução 1. Note que estamos calculando a interferência por enlace físico.

Se ao invés de escolhermos o comprimento de onda 2, escolhermos o comprimento de onda 3 para o caminho óptico 5-1, isto é, a solução #2. Não haverá mais interferência no enlace físico 6-1, pois d(1,3) = | 1 - 3 | =2, restando apenas a interferência dos caminhos virtuais de 2 para 4 nos enlaces físicos 2-3 e 3-4. Entretanto, se mudarmos também um dos caminhos virtuais de 2-4 para o comprimento de onda 3, teremos uma configuração sem nenhuma interferência entre canais (solução #3).

B) Adicionando restrições

- Para saber se ς é ativo no enlace m-n, criamos a variável binária $I_{mn\varsigma}$ e a adicionamos na formulação da seção 3 (problema RWA), então:

$$I_{mn\varsigma} = \begin{cases} 1 & se \quad \sum_{ij} p_{mn\varsigma}^{ij} \geq 1 \\ 0 & caso\ contrário \end{cases} \qquad (12)$$

Após isso, acrescentamos também a restrição de interferência de canal adjacente ao RWA, que deve ser menor que um limite pré-definido, o qual será associado à Relação Sinal-Ruído Óptica (OSNR), que é uma relação entre as potências de sinal e de ruído recebidas, sendo um parâmetro que também está associado à interferência entre canais. Para este propósito, implementamos as seguintes restrições para cada fibra:

$$I_{mn(\varsigma+1)} + I_{mn(\varsigma-1)} + \alpha * I_{mn\varsigma} \leq D_{mn} + \alpha \quad (13)$$

Onde:

- α = constante (utilizando valores altos, e.g. a =100).
- D_{mn} = interferência máxima aceitável de canais adjacentes que pode ser tolerada em cada enlace de fibra
- $I_{mn(\varsigma+1)} + I_{mn(\varsigma-1)}$: soma de comprimentos de onda que afetam o comprimento de onda ς. Somente os comprimentos de onda adjacentes contribuem para a interferência, daí a necessidade de (13), então:

$$\alpha * I_{mn\varsigma} = \begin{cases} \alpha & se\ \varsigma = 1\ (ativo) \\ 0 & senão \end{cases}$$

Note, que a restrição (13) limita a interferência em uma fibra, se quisermos limitar a interferência total de um caminho óptico podemos definir este limite como $D_{0SNR} \leq D_{mn}.H$, onde relembramos que H é o número total de enlaces físicos que um caminho óptico pode percorrer. Por exemplo, se um caminho óptico tem H=3 e a interferência máxima permitida em cada enlace de fibra é 1, temos $D_{0SNR} \leq D_{mn}.H$ =1.3=3, sendo este um limite superior para a interferência total permitida em cada caminho óptico.

Se analisarmos os casos acima, temos:

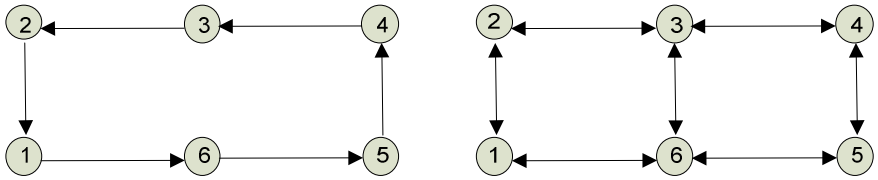
1. No caso de ocorrer $I_{mn\varsigma} = 1$ a restrição (13) se torna $I_{mn(\varsigma+1)} + I_{mn(\varsigma-1)} \leq D_{mn}$ e o número de comprimentos de onda que afetam o sinal está restrito a ser inferior ao limite pré-definido no enlace físico D_{mn}. Para uma tentativa de limitar o OSNR, Devemos observar que D_{0SNR} dependerá do número de enlaces físicos percorridos.
2. No caso de ocorrer $I_{mn\varsigma} = 0$, um comprimento de onda adjacente não foi selecionado e a restrição para canais adjacentes não afeta o RWA, desde que α seja suficientemente grande.
3. Casos extremos: se ς =1, $I_{mn(1-1)} = 0$; e se ς =W, $I_{mn(W+1)} = 0$.

5. Simulação e Resultados Numéricos

Para validar a formulação proposta consideramos duas redes pequenas (Figura 4). Uma rede em forma de anel, com seis nós (para mostrar uma simulação simples) e uma rede em malha de seis nós (para comparar com [Ramaswami e Sivarajan 1996] e [Krishnaswamy e Sivarajan 2007]). Também contemplamos uma rede maior: a rede de 14 nós da *National Science Foundation Network-NSFNET* (também de [Ramaswami e Sivarajan 1996] e [Krishnaswamy e Sivarajan 2007]), que devido à complexidade é planejada por meio de uma heurística.

A) Redes pequenas

Para as redes pequenas (Figura 4), resolvemos a MILP da seção 3 com as restrições adicionais da seção 4. Utilizamos o CPLEX 10.0, de [IBM/ILOG, 2009] em um Pentium IV, 2 Ghz. As soluções exatas são dadas nas Tabelas 3 e 4.



a) Rede em anel b) Rede em malha

Figura 4. Redes Pequenas

Tabela 2: Matriz de tráfego $T=(\lambda^{sd})$ para a rede de 6 nós, [Ramaswami e Sivarajan 1996]

-	0.537	0.524	0.710	0.803	0.974
0.391	-	0.203	0.234	0.141	0.831
0.060	0.453	-	0.645	0.204	0.106
0.508	0.660	0.494	-	0.426	0.682
0.480	0.174	0.522	0.879	-	0.241
0.950	0.406	0.175	0.656	0.193	-

Para a Figura 4a, com W=4, Δ=2 e T dada na Tabela 2, sem permitir qualquer interferência de enlace, D_{mn} = 0, a Tabela 3a mostra um possível VTD e RWA. O congestionamento é 3.67 e alguns possíveis enlaces virtuais não puderam ser estabelecidos; dos 12 possíveis, ($\Delta.N$), apenas 10 puderam ser configurados. Isso se deve ao fato de que, para o grau virtual 2, precisamos de mais comprimentos de ondas, ou deveremos permitir alguma interferência para configurar todos os possíveis caminhos ópticos. Para a mesma rede, com os mesmos parâmetros anteriores, mas permitindo interferência ilimitada, o congestionamento é de 2.45 (Tabela 3b). Nesse caso, todos os caminhos ópticos foram configurados. Logo, deve haver um compromisso entre números de comprimentos de ondas disponíveis, congestionamento máximo permitido ou capacidade do canal e limitação da interferência, baseada na disponibilidade de recursos e maximização de atendimento.

Tabela 3. Soluções para rede pequena em anel

a) Solução sem interferência

W=4, Δ=2 , D_{mn}=0

b_{ij}	*Rota*	ς_i	λ_{max}
1-5	1-6-5	3	3.67
1-6	1-6	1	
2-1	2-1	3	
3-1	3-2-1	1	
3-2	3-2	4	
5-3	5-4-3	3	
4-3	4-3	1	
5-3	5-4-3	3	
5-4	5-4	1	
6-5	6-5	1	

b) Solução com interferência ilimitada

W=4, Δ=2 , D_{mn}=ilimitada

b_{ij}	*Rota*	ς_i	λ_{max}
1-5	1-6-5	2	2.45
1-6	1-6	1	
2-1	2-1	1	
2-6	2-1-6	4	
3-1	3-2-1	2	
3-2	3-2	1	
4-2	4-3-2	4	
4-3	4-3	2	
5-3	5-4-3	1	
5-4	5-4	2	
6-4	6-5-4	1	
6-5	6-5	4	

Para a Figura 4b, a matriz de tráfego T da Tabela 2 também foi usada. Consideramos quatro parâmetros: D_{mn}, H, W e Δ. Os resultados estão na Tabela 4 e "*" indica que não há restrição para aquele parâmetro particular naquela coluna. Com esses parâmetros, muitas combinações são possíveis. Nós apresentamos resultados para algumas

combinações e comparamos com os resultados de [Krishnaswamy e Sivarajan 2007]. Para Δ=2, W=2, H=2 e D_{mn}=0 o congestionamento é 2.21. Ou seja, o mesmo obtido com permissão total de interferência, que é o caso considerado em [Krishnaswamy e Sivarajan 2007]. Se não impusermos qualquer restrição a W e H, mas não permitirmos interferência, também obtemos o mesmo resultado de [Krishnaswamy e Sivarajan 2007]. Para o grau 3 e W=2, na formulação tradicional, o congestionamento é 1.183. Porém, com D_{mn}=0 (sem interferência) o congestionamento sobe para 2.21. No entanto, se houver disponibilidade de mais um comprimento de onda, W=3, o congestionamento é similar nas duas formulações. A análise dos resultados para os graus 4 e 5 têm explanações similares às dos graus menores.

Tabela 4. Comparação com [Krishnaswamy e Sivarajan 2007]

Parâmetros			Nova Formulação		[Krishnaswamy e Sivarajan 2007]	
Δ	W	H	D_{mn}	λ_{max}	D_{mn}	λ_{max}
2	2	2	0	2.21	*	2.21
2	*	*	0	2.04	*	2.04
3	2	*	0	2.21	*	1.18
3	*	*	0	1.18	*	1.18
4	3	*	0	1.10	*	0.89
4	*	*	0	0.89	*	0.89
5	4	*	0	1.11	*	0.71
5	*	*	0	0.71	*	0.71

"*" significa que não há restrições quanto a disponibilidade de recursos ou que D_{mn} é ilimitada

B) Redes Grandes - Estratégia Heurística

Os problemas VTD e PTD descritos anteriormente são complexos e cada um deles é conhecido como *NP-Hard* [Ramaswami *et al*, 1996], ou seja, o tempo de execução do problema cresce de maneira exponencial quando o número de variáveis aumenta. Logo, se cada um dos problemas é NP, a solução dos dois conjuntamente é ainda mais complexa. Então, a divisão em VTD e PTD é aceitável porque diminui esta complexidade. Entretanto, para uma maior eficiência do uso dos recursos da rede sob uma perspectiva de integração dos planos de controle da camada óptica (PTD) e da camada cliente (VTD), o interessante é encontrar uma maneira para resolver estes problemas de forma integrada e num tempo computacional aceitável. Para isto, buscamos uma estratégia heurística para tornar o problema com muitas restrições aceitável, mas que evidentemente não fornecerá a solução ótima.

Heurística VTD/PTD

Passo 1: Dada a matriz de tráfego estático T= (λ^{sd}) e o grau virtual Δ encontrar a configuração dos enlaces virtuais (b_{ij}) com uma heurística tradicional para resolver o VTD. (Neste trabalho, utilizamos a Busca Tabu. [Santos e*t al*, 2007]. Formando assim a topologia virtual G_v.

Passo 2: Com a formulação VTD da Seção 3, rotear o tráfego T= (λ^{sd}) nos b_{ij}'s da topologia virtual estabelecida no Passo anterior, encontrando o min λ_{max}.

Passo 3: Dado a topologia virtual *Gv* encontrada no Passo anterior, a topologia física G_f, e o número de comprimentos de onda disponíveis W . Se não desejar interferência vá para o Passo 4 e chame-o de Heur I (interferência limitada). Caso contrário, vá para o Passo 5 e chame-o de Heur II (com interferência).

Passo 4 (interferência limitada -Heur I): Resolva o RWA com a nova formulação, apenas PTD, acrescentando as restrições de interferência, definindo limites para D_{mn} e consequentemente D_{OSNR}; use o roteamento por caminhos mais curto como função objetivo do PTD. Ir para o Passo 6.

Passo 5 (com interferência- Heur II): Resolva o RWA com a formulação tradicional, PTD sem restrições de interferência, use o roteamento por caminhos mais curto como função objetivo do PTD. Evidentemente, podemos usar neste Passo as restrições de interferência, mas fazendo D_{mn} ilimitada. Ir para o Passo 6.

Passo 6: Se o RWA é viável, mostre o valor de λ_{max} e finalize. Caso contrário, o problema completo é inviável (mostre "X") e finalize.

Nota: – as soluções b_{ij} para Heur I e Heur II são as mesmas. Por isso, esperamos resultados semelhantes para o congestionamento nas soluções viáveis; – a inviabilidade é caracterizada pela insuficiência de comprimentos de onda para atender a condição de planejamento escolhida.

Nós aplicamos a heurística acima para a rede NSFNET, apresentada em [Ramaswami e Sivarajan, 1996] que tem 14 nós e 21 arcos. O par de arcos direcionais representa um par de fibras, uma em cada direção. A Tabela 5 apresenta os resultados heurísticos para a matriz P1 de tráfego, também de [Ramaswami e Sivarajan, 1996].

Na Tabela 5, há duas colunas vizinhas, a saber: grau virtual Δ e número de comprimentos de onda disponíveis W, que são parâmetros para Heur I e Heur II. Relembrando que o símbolo "*" significa que não há restrições quanto a disponibilidade de um dado parâmetro. A coluna do congestionamento, para Heur I e Heur II, mostrará o resultado se a solução for viável. Para comparar com estratégias que não levam em conta a interferência (interferência ilimitada) consideramos nossa formulação com D_{mn}=0 para Heur I e consequentemente D_{OSNR}=0; e D_{mn}= ilimitada para Heur 2, e consequentemente D_{OSNR}= ilimitada. Para o grau virtual 2, na primeira linha, com W= 2 a solução de Heur I é inviável. Contudo, se aumentarmos o número de comprimentos de onda disponíveis para 3, encontramos uma solução viável, com congestionamento 553.76. Podemos observar também que para esse conjunto de parâmetros, 3 é um limite inferior no número de comprimentos de onda necessários. Então, para encontrarmos soluções sem qualquer interferência, precisamos utilizar $W \geq 3$. Para os mesmos parâmetros a Tabela 5 também mostra os resultados de Heur II, sem considerar qualquer limite na interferência, e verifica-se que uma solução viável pode ser encontrada. A questão que se deve observar é a seguinte: utilizar mais recursos (comprimentos de onda) em prol da eliminação da interferência ou minimizar o uso de recursos, permitindo interferências que podem degradar o sinal? Esta é uma questão que depende de disponibilidade de recursos do planejador e nível de degradação permissível para o sinal. Para outros graus, a discussão é semelhante.

A Figura 6 mostra o número de comprimentos de onda necessários para tornar viáveis as soluções para vários graus. Nesta figura, para a Heur I, mais uma vez D_{mn}=0. Por exemplo, para o grau 5 precisamos de 7 comprimentos de onda para realizar uma solução viável com a Heur I. Com a Heur II, para o mesmo grau, necessitamos apenas de 5 comprimentos de onda, mas com interferência ilimitada. Também obtemos resultados da heurística que resolve o VTD/PTD de uma rede óptica, a HLDA (*Heuristc Logical Topology Design Algorithm*) de [Ramaswami e Sivarajan 1996], que computa o número de comprimentos de onda com interferências ilimitadas, para comparação com as heurísticas apresentadas neste trabalho. As melhores soluções obtidas pela Heur I podem ser vistas na Figura 6, pois esta utiliza menos comprimentos de onda e não permite qualquer interferência, quando comparada com a HLDA.

Tabela 5. Solução para rede maior. (NSFNET com 14 nós)

Δ	W	*Heur I* $D_{mn}=0$ λ_{max}	*Heur II* D_{mn}=*Ilimitada* λ_{max}
2	2	X	553.76
2	3	553.76	553.76
2	*	553.76	553.76
5	5	X	63.25
5	6	X	63.25
5	7	63.25	63.25
5	*	63.25	63.25
7	7	X	43.77
7	8	X	43.77
7	9	X	43.77
7	10	X	43.77
7	11	43.77	43.77
7	*	43.77	43.77
10	11	X	28.35
10	12	X	28.35
10	13	X	28.35
10	14	X	28.35
10	15	X	28.35
10	16	X	28.35
10	17	X	28.35
10	18	X	28.35
10	19	28.35	28.35
10	*	28.35	28.35

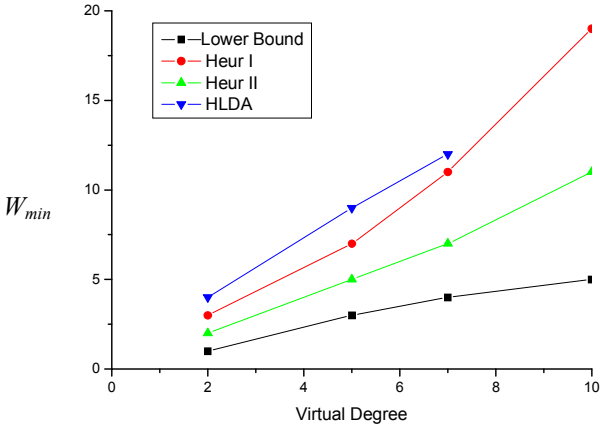


Figura 6. Número de comprimentos de onda necessários (W_{min}), em função do grau virtual. O *Lower Bound* foi obtido de [Ramaswami and Sivarajan 1996])

6. Conclusões

Os experimentos computacionais demonstram claramente que a formulação linear proposta apresenta uma melhora em relação às estratégias tradicionais, quando queremos evitar a interferência entre canais. Essa melhora vem do fato de que as formulações e os algoritmos existentes na literatura selecionam as rotas de modo a otimizar parâmetros da camada da rede, como por exemplo, o número de enlaces percorridos de uma fonte para o destino ou o balanceamento do tráfego na rede. Entretanto, pouca análise é feita com relação a interferência que pode ocorrer em canais adjacentes, o que degrada a qualidade do sinal no receptor. Nos exemplos demonstrados, verifica-se que a formulação bloqueia a alocação de canais adjacentes em custa do aumento do número de comprimentos de ondas utilizados. No entanto, nas redes ópticas operacionais há disponibilidade de muitos comprimentos de ondas para fazer o planejamento. É fato que a não regeneração do sinal óptico em nós intermediários de redes ópticas transparentes faz com que a qualidade do sinal se degrade. Portanto, a alocação de comprimentos de onda levando em conta esse fator pode ajudar os planejadores e operadores de rede a oferecer uma melhor QoS aos clientes. As perdas inerentes aos componentes ópticos (comutadores ópticos, multiplexadores, demultiplexadores etc) também afetam a qualidade do sinal e serão objetos de estudos futuros, assim como o estudo de redes mais complexas, para assim termos uma formulação mais robusta.

Referências

Assis, K.D.R.; Giozza, W.F. e Waldman, H. (2005) "WDM Optical Networks: A Complete Design". Journal of Communication and Information Systems, Vol. 20, No. 3, pp. 81-95.

Assis, K.D.R; Savasini, M.; Waldman. H. (2009) “How Many Lightpaths we need Today and How Many Lightpaths we will need Tomorrow” Journal of Optical Communications. vol. 30, issue 3, 176 – 179.

Azodolmolky, Siamak., Klinkowski , Mirosław., Marin, Eva., Careglio , Davide., Pareta , Josep Solé., Tomkos, Ioannis (2009) “A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks” Computer Networks, vol. 53 pp. 926–944.

Banerjee, D. and Mukherjee, B., (1996) "A Practical Approach for Routing and Wavelength Assignment in Large Wavelength-Routed Optical Networks", JSAC, vol. 14, n.5, pp. 903-908.

Bastos Filho, C. J. A. ; Chaves, D. A. R. ; Silva, F. S. F. ; Carvalho, R. V. B. ; Pereira, H. A. ; Martins-Filho, J. F. (2009) “Wavelength Assignment Optimization for All-Optical Networks Using Evolutionary Computation” XXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, v.1. pp 31-44, Recife/PE.

Byrav Ramamurthy, Debasish Datta, Helena Feng, Jonathan P. Heritage, and Biswanath Mukherjee (1999) “Impact of Transmission Impairments on the Teletraffic Performance of Wavelength-Routed Optical Networks” Journal of Lightwave Technology, Vol. 17, Issue 10, pp. 1713-.

Deng, T., Subramaniam, S. e Xu, J., (2004) "Crosstalk-Aware are Wavelength Assignment in Dynamic Wavelength Routed Optical Networks", *Broadnets 2004*. First International Conference on Broadband Networks.

Dutta, R. e Rouskas, G., (2000) “A Survey of Virtual Topology Design Algorithms for Wavelength Routed Networks”, Optical Networks (SPIE) Vol 1, No 1, pp. 73-89, Jan.

He, J., Brandt-Pearce, M. etal, (2007) "QoT-Aware are Routing in Impairment-Constrained Optical Networks" IEEE GLOBECOM, pp. 2269-2274, Nov.

IBM/ILOG/CPLEX, (2009); http://www.ilog.com

Jaumard, B., Meyer, C., Thiongane, B. (2009)”On column generation formulations for the RWA problem”, Elsevier Discrete Applied Mathematics. Volume 157 , Issue 6 March.

Jaumard, B., Meyer, C. and Thiongane, B., (2007) “Comparison of ILP formulations for the RWA problem” . Elsevier Optical Switching and Networking. v4 i3-4. 157-172.

Krishnaswamy, R.M. e Sivarajan, K.N., (2001) " Design of logical topologies: A linear formulation for wavelength routed optical networks with no wavelength changers ", IEEE Trans. on Networking, vol. 9, no. 2, pp. 186 186-198.

Manousakis, K., Christodoulopolos, K. e Varvarigos, E., (2008) “Avoiding Adjacent Channel Interference in Statatic RWA”, CSNDSP08.

Pavon-Marino, Pablo., Aparicio-Pardo, Ramon., Garcia-Manrubia, Belen and Skorin-Kapov, Nina., (2009) “Virtual topology design and flow routing in optical networks under multihour traffic demand”, Photonic Network Communications, August. Springer Netherlands.

Ramaswami, R. e Sivarajan, K.N., (1996) “Design of Logical Topologies for Wavelength-Routed All Optical Networks”. IEEE/JSAC, vol. 14, pp. 840-851. Junho.

Ramaswami, R., (2006) “Optical Networking Technologies: What Worked and What Didn´t”. IEEE Communications Magazine, Sept, pp 132-139.

Santos, A. F.; Giozza, William; Assis, K.D.R. (2007) “Meta-Heurística Tabu Search para o Planejamento de Redes Ópticas WDM” V Escola Regional de Redes de Computadores- ERRC, Santa Maria-RS.

Zang, H., Jue, J.P. e Mukherjee, B., (2000) “A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed optical WDM Networks”, Optical Networks Magazine, vol.1, pp. 47-60, Janeiro.

XV Workshop de Gerência e Operação de Redes e Serviços

♦

Sessão Técnica 3

Gerenciamento de Serviços e Aplicações

Similaridade para Avaliação de Riscos em Planos de Mudança de TI

Luis Armando Bianchin[1], Juliano Araujo Wickboldt[1], Ricardo Luis dos Santos[1], Roben Castagna Lunardi[1], Bruno Lopes Dalmazo[1], Fabricio Girardi Andreis[1], Weverton Luis da Costa Cordeiro[1], Abraham Lincoln Rabelo de Sousa[1], Lisandro Zambenedetti Granville[1], Luciano Paschoal Gaspary[1]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS
{labianchin, jwickboldt, rlsantos, rclunardi, bldalmazo, fgandreis, wlccordeiro, rabelo, granville, paschoal}@inf.ufrgs.br

Abstract. *The proper management of IT infrastructures is essential for organizations that aim to deliver high quality services. Given the dynamics of these environments, changes become imminent. In some cases these changes might raise failures that may cause disruption to services affecting the business continuity, which makes necessary the evaluation of the risks associated with changes before their actual execution. Taking advantage of information from past deployed changes it's possible to estimate the risks for recently planned ones. Thereby, in this paper, we propose a solution to weigh the information available from past executed changes by the similarity calculated in relation with the analyzed change. A prototype system was developed in order to evaluate the efficacy of the solution in an emulated IT infrastructure. The results show that the solution is capable of capturing similarity among changes, improving the accuracy of risk assessment for IT change planning.*

Resumo. *O gerenciamento apropriado de infra-estruturas de TI é fundamental para organizações que buscam oferecer serviços de alta qualidade. Dada a dinâmica desses ambientes, mudanças tornam-se iminentes. Em alguns casos as mudanças causam falhas que podem afetar a disponibilidade dos serviços afetanto a continuidade do negócio, o que torna necessário avaliar os riscos associados a essas mudanças antes que sejam executadas. Utilizando-se informações de mudanças implantadas anteriormente é possível estimar os riscos de mudanças recém planejadas. Para isso, neste trabalho, é proposta uma solução para ponderar os dados disponíveis sobre mudanças passadas pela similaridade que possuem em relação à mudança analisada. Um protótipo foi desenvolvido a fim de avaliar a eficácia da solução numa infra-estrutura de TI emulada. Os resultados mostram que a solução é capaz de capturar similaridade entre diferentes mudanças, melhorando a precisão das estimativas de risco no planejamento de mudanças.*

1. Introdução

Organizações que buscam oferecer serviços de alta qualidade normalmente precisam tratar o aumento de tamanho e complexidade de suas infra-estruturas de tecnologia da informação (TI). Infra-estruturas modernas incluem Itens de Configuração (ICs) que variam

de elementos físicos como servidores, estações de trabalho, dispositivos móveis e roteadores, a elementos lógicos como pacotes de *software* e serviços de rede. A fim de auxiliar tais organizações a empregar um gerenciamento racional de suas infra-estruturas de TI, o *Office of Government Commerce* (OGC) introduziu o *Information Technology Library* (ITIL) [ITIL 2009]. O ITIL apresenta essencialmente de um conjunto de boas práticas e processos cujo objetivo é guiar o gerenciamento apropriado de recursos e serviços de TI.

O *gerenciamento de mudanças* é um dos principais tópicos abordados pelo ITIL e que define como mudanças devem ser conduzidas numa infra-estrutura de TI. O ITIL define que mudanças devem ser especificadas de forma declarativa, em documentos chamados *Requests for Change* (RFCs). Tais RFCs devem então ser processadas, manual ou automaticamente, a fim de gerar Planos de Mudança (PM), os quais são *workflows* de ações que, quando executados, levarão a infra-estrutura de TI gerenciada a um novo estado funcional que será consistente com as mudanças originalmente expressas na RFC. Porém, devido a problemas imprevisíveis que podem ocorrer durante o desenrolar das mudanças, os quais podem causar interrupções nos serviços da infra-estrutura de TI, é conveniente avaliar os riscos associados aos PM antes de sua execução sobre a infra-estrutura gerenciada.

A avaliação de risco em gerenciamento de mudanças de TI é uma área de pesquisa recente que apresenta desafios bastante interessantes. Um deles, sendo de especial interesse na pesquisa apresentada neste artigo, reside no fato de que metodologias de estimativa de riscos em mudanças utilizando abordagem baseadas na análise dos históricos de execuções passadas de PMs requerem a execução recorrente de um mesmo PM para que se possa extrair resultados relevantes. No caso de PMs recém especificados, ou seja, sem histórico de execuções para avaliação, tal cômputo não seria viável. Isso conduz a situação em que PMs definidos para mudanças nunca executadas anteriormente não podem ter seu potencial de afetar os recursos de TI observados; operadores de TI não têm alternativa exceto executar os novos PMs e lidar de forma reativa com os problemas que podem vir a ocorrer durante a execução.

Neste trabalho, porém, argumentamos que a avaliação de risco pode ainda ser feita se os riscos de novos PMs forem computados considerando execuções passadas de PMs *similares*. Assim, neste trabalho é investigada uma solução para medir a similaridade entre atividades de PMs. Nossa abordagem consiste em comparar as atividades de um novo PM de interesse com as atividades de PMs já empregados anteriormente na infra-estrutura de TI gerenciada, e assim selecionar atividades similares através do uso de um algoritmo específico para este fim. Em seguida, execuções passadas dos PMs existentes são observadas, ponderadando-as pelas similaridades encontradas, e assim permitindo uma estimativa com maior precisão da probabilidade de falha das atividades do novo PM. A solução foi avaliada em um estudo de caso conduzido sobre uma infra-estrutura de TI emulada, a fim de avaliar seu pontecial em capturar atividades similares.

O restante deste artigo está organizado da seguinte forma. Na Seção 2 são apresentados os trabalhos relacionados ao tema desta pesquisa. Na Seção 3 alguns conceitos e definições usados na solução são explicados. A solução proposta é detalhada na Seção 4. Na Seção 5 um estudo de caso é desenvolvido usando a abordagem introduzida na seção anterior. Finalmente, na Seção 6 o artigo é concluído com considerações finais e indicações de trabalhos futuros.

2. Trabalhos Relacionados

Gerenciamento de risco é um tópico que tem sido amplamente discutido em áreas tão diversas quanto engenharia, medicina e economia. Risco é um conceito relacionado com o potencial de eventos incertos ocorrerem, normalmente com efeitos negativos, que afetam a realização dos objetivos dos negócios [Office of Government Commerce 2007]. Especialmente em gerenciamento de mudanças, risco é um aspecto importante que deve ser analisado, já que mudanças mal implementadas podem resultar em falhas que causam interrupções em serviços críticos para a continuidade dos negócios. Para promover a análise de riscos em gerenciamento de mudanças, as boas práticas do ITIL [ITIL 2007] sugerem que riscos devem ser avaliados e mitigados antes de uma mudança ser aprovada, reduzindo assim tanto a chance de ocorrer eventos negativos como também minimizando o impacto que esses eventos podem ter sob a infra-estrutura gerenciada.

Setzer *et al.* [Setzer *et al.* 2008] e Sauvé *et al.* [Sauvé *et al.* 2007] pesquisaram sobre a análise de risco no processo de planejamento do agendamento da execução de RFCs. Guiados por objetivos de negócios, a abordagem dos autores baseia-se na determinação de prioridades de execução de RFCs potencialmente concorrentes, com o objetivo de minimizar os riscos e os custos de implantação sobre os serviços das empresas. De acordo com os autores, o tempo elevado de indisponibilidade nos serviços durante a implantação de mudanças pode prejudicar severamente os serviços de negócio. Assim, são analisadas estratégia de implantação de RFCs considerando o impacto que cada RFC do conjunto pode ter sobre o negócio.

Em outro trabalho, Wickboldt *et al.* [Wickboldt *et al.* 2009b], a fim de permitir eventuais ajustes em uma RFC antes de sua aprovação, propuseram uma solução para avaliar os riscos já na fase de planejamento de mudanças, considerando tanto a probabilidade de ocorrerem falhas quanto a relevância dos elementos da infra-estrutura de TI envolvidos, o que permite compreender também o impacto de eventuais falhas. Para a estimativa de probabilidade de falhas, os autores usaram registros de execuções passadas como mecanismo para encontrar PMs suficientemente parecidos com o PM que estava em análise, levando-se em conta informações como a quantidade de falhas e execuções, além da similaridade dos planos envolvidos. Neste trabalho, porém, a busca por PMs similares foi realizada de forma extremamente rudimentar, sem considerar aspectos importantes que permitiram identificar similaridades de forma mais adequada.

Na tentativa de se determinar mais precisamente a similaridade entre *workflows* de mudanças, estes poderiam ser modelados como grafos dirigidos e então terem sua similaridade computada a partir de técnicas já utilizadas em grafos, como por exemplo no trabalho de Chartrand *et al.* [Chartrand *et al.* 1998]. Tais técnicas visam atingir o isomorfismo entre os grafos a partir da verificação da quantidade de operações necessárias, sobre e arcos e nodos, para transformar um grafo em outro. Porém, além de serem mais complexas, essas técnicas buscam uma comparação considerando apenas nodos e arcos, não levando em conta aspectos semânticos fundamentais em *workflows* de mudança, como a seqüencialidade e paralelismo entre atividades.

Outros autores investigaram a similaridade entre *workflows* considerando noções de equivalência de traço - como na pesquisa de Hidders *et al.* [Hidders *et al.* 2005] - e bissimulação - como proposto por Van der Aalst *et al.* [Van der Aalst e Basten 2002]. Porém, tais equivalências não são aplicáveis ao contexto de nossa pesquisa porque ofere-

cem uma resposta com granularidade muito baixa; ou *workflows* são equivalentes ou não são. Outras pesquisas, como as de Van Dongen *et al.* [Van Dongen *et al.* 2008] e Van der Aalst *et al.* [Van der Aalst *et al.* 2006], investigaram a similaridade de *workflows* de processos considerando os logs de execução para comparar o comportamento dos *workflows* analisados. Tal abordagem, porém, não se aplica ao contexto de avaliação de risco porque ainda não se sabe o comportamento do novo PM que está sendo analisado ao ser executado; na realidade pretende-se prever qual será o seu comportamento quando o PM for executado.

Por fim, Wombacher e Rozie [Wombacher e Rozie 2006] compararam vários métodos de similaridade aplicáveis a autômatos e grafos, avaliando seu uso em *workflows*. Seguindo essa linha de pesquisa, Li *et al.* [Li *et al.* 2008] propuseram uma medida de similaridade de modelos de processos em que usa-se técnicas de lógica digital para calcular esse escore. Porém, mesmo que PMs sejam compostos de *workflows*, é importante analisar o detalhamento das atividades que compõem estes *workflows*, dando importância também aos participantes envolvidos nas atividades. Desse modo, faz-se necessário construir uma solução para cálculo de similaridade que leve em conta também outros aspectos que favoreçam o contexto de análise de risco.

3. Definições

A fim de fornecer embasamento teórico à solução proposta neste trabalho, inicialmente, nesta seção, são revisados e formalizados alguns conceitos importantes propostos em trabalhos anteriores. Além disso, são introduzidos alguns novos conceitos utilizados na solução que será apresentada na seção seguinte.

3.1. Atividade

Uma atividade descreve uma única operação envolvendo elementos de *software*, *hardware* e demais Itens de Configuração (ICs), que pode ser realizada de forma automatizada ou manual - nesse caso envolvendo humanos - e cujo objetivo é modificar os ICs de forma a contemplar as mudanças descritas em uma RFC. As atividades são organizadas nos PMs na forma de um *workflow* que determina: a ordem de execução das atividades, restrições temporais entre elas e possíveis paralelismos. As operações executadas pelas atividades afetam os seus participantes, por exemplo, ao se instalar ou remover pacotes de *software* em computadores, ao se alterar as configurações de roteadores ou ao se editar as regras de *firewall*. No caso de atividades manuais, recursos humanos também são associados às atividades na forma de participantes.

Neste trabalho, uma atividade é formalizada como uma tupla: $A = \langle \Omega, \lambda \rangle$, onde:

- Ω é a operação realizada pela atividade (*e.g.*, instalação, atualização, desinstalação e configuração);
- λ é o conjunto de elementos participantes da atividade (*e.g.*, humanos, elementos de *hardware*, *software* e demais ICs).

3.2. Tipos de Falha

Para todos os PMs implantados sobre a infra-estrutura de TI, é armazenado o registro (*log*) das atividades executadas. Esses registros contêm os traços de execução dos PM, permitindo a posterior recuperação das informações do *workflow* e a ordem em que as

atividades foram executadas. Além disso, é possível extrair dos *logs* informações sobre o êxito ou fracasso das execuções e, quando há falhas, estas são classificadas em seis categorias ou Tipos de Falha (TF) [Wickboldt *et al.* 2009c]: (*i*) Falha de Atividade (FA), (*ii*) Falha de Recurso (FR), (*iii*) Falha de Humano (FH), (*iv*) Falha de Tempo (FT), (*v*) Intervenção Externa (IE) e (*vi*) Violação de Restrição (VR).

Um aspecto importante ao se classificar falhas ocorridas em mudanças é que dessa forma se permite associar uma falha ao IC que a ocasionou. Por exemplo, considerando o caso de uma atividade de instalação de *software* sobre um determinado computador; se a falha ocorrida é uma FA, diz-se que o elemento que a provocou foi o *software*, enquanto que se a falha é classificada como FR (Falha de Recurso), esse evento ficará associado ao *hardware*. Como o foco deste trabalho está no cálculo da *similaridade* de PMs, e também por medida de simplificação, serão consideradas apenas Falha de Atividade (FA), que são ocasionadas por problemas inerentes às atividades do PM, tais como exceções geradas durante a instalação ou configuração de um software. Informações sobre os outros cinco Tipos de Falha (TF) são descritas no trabalho de Wickboldt *et al.* [Wickboldt *et al.* 2009c].

Neste trabalho, considera-se que as mudanças realizadas sobre a infra-estrutura de TI são controladas e documentadas conforme as recomendações feitas pelo ITIL. Em trabalhos passados deste grupo de pesquisa, uma solução fim-a-fim de sistema de planejamento e execução de mudanças foi proposta [Cordeiro *et al.* 2008, Wickboldt *et al.* 2009a]. Com auxilio de um sistema como esse, é possível manter de forma organizada o histórico das mudanças realizadas sobre cada CI. A detecção e tratamento de falhas ocorridas durante as mudanças estão fora do escopo deste trabalho, porém é importante que esses eventos sejam devidamente documentados, seja este um processo automatizado ou executado manualmente durante a revisão das mudanças, a fim de permitir futuras estimativas de riscos.

3.3. Workflow Influencial

Chamamos Workflow Influencial o subconjunto de atividades de um *workflow* que podem influenciar a execução de uma dada atividade dentro de um mesmo PM. Considera-ses neste trabalho que uma atividade A pode influenciar a execução (eventualmente também as falhas) de outra atividade B quando: (*i*) A antecede B no *workflow*, ou seja, para que B possa ser executada A deve ter sido concluída primeiro, ou (*ii*) A está em paralelo com B, sendo assim a ordem suas execuções não é determinística.

Intuitivamente, no que diz respeito à análise de riscos, o primeiro caso captura situações em que a falha de uma atividade B foi causada indiretamente por problemas ocorridos em atividades que a antecederam, enquanto que o segundo caso captura problemas ocasionados por execuções em paralelo onde pode haver, por exemplo, disputa por recursos compartilhados. Em outras palavras, o Workflow Influencial é o próprio *workflow* excetuando as atividades que ocorrem após uma dada atividade, já que a execução dessa atividade não pode receber interferência das atividades que vêm a seguir. Além disso, a atividade objeto da análise também é incluída no seu Workflow Influencial juntamente com as atividades que a antecedem ou estão em paralelo com ela. Ademais, as transições entre as atividades do *workflow* original são preservadas no Workflow Influencial.

3.4. Similaridade

Uma métrica de similaridade objetiva estimar quão parecidas duas entidades de qualquer natureza são. Basicamente, existem duas propriedades relacionadas com as medidas de similaridade que são muito interessantes para a solução descrita na próxima seção:

- **Comutatividade:** determina que o valor de similaridade entre X e Y é igual ao valor de similaridade de Y e X;
- **Intervalo de 0 a 1:** o escore de similaridade varia de 0, totalmente diferentes, a 1, exatamente iguais.

Métricas de cálculo de similaridade que comumente respeitam essas propriedades são as utilizadas para comparação de *strings*, as quais são largamente empregadas para encontrar semelhanças entre textos, análises de DNA, mineração de dados, entre outros fins. Um conceito muito utilizado no cálculo de similaridade de *strings* que vem a ser bastante importante para a solução proposta neste trabalho é o conceito de distância. Basicamente, a distância entre duas entidades representa o número de operações básicas para transformar uma entidade noutra. De fato, existem diferentes medidas de distância de *strings*. Em particular, cabe ressaltar a distância de edição (ou Distância de Levenshtein) entre duas palavras que representa a menor quantidade de inserções, substituições e supressões de símbolos para transformar uma palavra em outra [Levenshtein 1966]. Usando um valor de distância d, a similaridade pode ser obtida subtraindo-se este valor a partir da diferença máxima entre as duas entidades m e dividindo por essa diferença máxima, ou seja, $sim = \frac{m-d}{m}$ [Wombacher e Rozie 2006].

Já para cálculo de coeficiente de similaridade entre conjuntos, outras métricas também foram estudas [Cohen *et al.* 2003], como Jaccard, MongeElkan [Monge e Elkan 1996] e SoftTFIDF. Em especial, convém detalhar o funcionamento do índice de Jaccard: a partir de dois conjuntos C_1 e C_2, pode-se calcular o escore de similaridade pela relação entre o número de elementos comuns e a quantidade total de elementos em ambos os conjuntos.

$$sim\_jaccard = \frac{|C_1 \cap C_2|}{|C_1 \cup C_2|} \quad (1)$$

O índice de Jaccard (Equação 1), bem como os demais conceitos e definições descritos nesta seção, servem de base para a solução de cálculo de similaridade em planos de mudança apresentada no seguimento deste artigo.

4. Solução Proposta

A solução para cálculo de similaridade proposta neste artigo é capaz de analisar um *workflow*, atividade por atividade, encontrando dentro de uma base de dados de *workflows* (*e.g.*, uma base de dados de PMs previamente executados) atividades similares às analisadas considerando dois aspectos: (*i*) a similaridade entre as duas atividades e seus participantes, chamada neste artigo de Similaridade Pontual e (*ii*) a similaridade dos Workflows Influenciais de ambas as atividades a fim de capturar a similaridade do contexto ou ambiente em que foram executadas, chamada de Similaridade de Workflows.

A Figura 1 apresenta o fluxo de informações utilizado pela solução desde a leitura do *workflow* a ser analisado, a seleção das atividades similares a partir dos Registros de Execução, o processamento dessas informações, até a composição de um relatório com os resultados da análise de similaridade das atividades. Os algoritmos que realizam os cálculos de similaridade são apresentados na continuação desta seção.

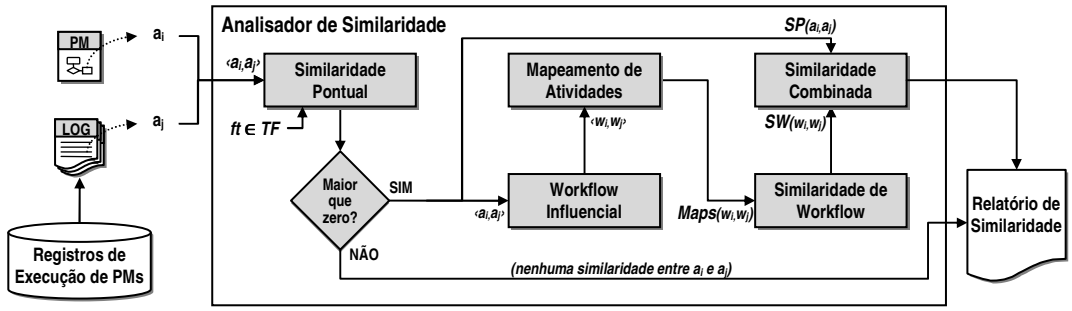


Figura 1. Fluxo de Informações da Solução

4.1. Similaridade Pontual

Usando a definição de atividade (Seção 3.1), pode-se estabelecer um algoritmo para comparar isoladamente duas atividades e determinar quão similares estas são no que diz respeito a operação realizada e participantes envolvidos. A esse algoritmo é atribuído o nome de Similaridade Pontual (SP).

Algoritmo 1 SIMILARIDADEPONTUAL

Entradas: Atividades $a_1 = \langle \Omega_1, \lambda_1 \rangle$ e $a_2 = \langle \Omega_2, \lambda_2 \rangle$, e um tipo de falha $ft \in TF$
Saídas: Similaridade Pontual das atividades a_1 e a_2 segundo o tipo de falha ft

1: **se** $\Omega_1 \neq \Omega_2$ **então**
2: $\quad SP \leftarrow 0$
3: **senão se** elementos do tipo ft de a_1 e a_2 são diferentes **então**
4: $\quad SP \leftarrow 0$
5: **senão**
6: $\quad SP \leftarrow \frac{|\lambda_1 \cap \lambda_2|}{|\lambda_1 \cup \lambda_2|}$
7: **fim se**
8: **retorna** SP

Obtém-se esse escore de SP a partir do Algoritmo 1, o qual se baseia fortemente no conceito de similaridade de Jaccard. Basicamente, para que duas atividades sejam significativamente relacionadas, elas devem executar a mesma operação (Linha 1) e possuir os mesmos participantes relacionados ao tipo de falha analisado (Linha 3), caso contrário, podemos afirmar que a SP entre essas atividades é zero, ou seja, são completamente diferentes. Caso contrário, o escore de similaridade será a razão entre a quantidade de participantes em comum e o total de participantes envolvidos em ambas as atividades, ou seja, Jaccard aplicado aos conjuntos de participantes de ambas as atividades (Linha 6). Assim, por exemplo, ao analisar a similaridade considerando Falhas de Atividade (FA), apenas execuções de atividades que realizam as mesmas operações sobre os mesmos elementos de *software* serão capturadas. É importante lembrar que neste trabalho são consideradas apenas FA, porém no algoritmo, ft pode assumir qualquer valor para um Tipo de Falha (descritos na Seção 3.2) pertencente a um conjunto TF. Sendo assim, para contemplar outros Tipos de Falha seria necessário repetir o mesmo algoritmo para cada um deles.

Na solução apresentada nesta seção, a SP determina o grau de semelhança entre as operações e os participantes de duas atividades. Sendo assim, na análise de riscos de Planos de Mudança a SP é utilizada para capturar as atividades relacionadas a partir

dos Registros de Execução. Isto é, caso a SP de duas atividades seja igual a zero, não é necessário executar nenhum dos outros algoritmos e as atividades são imediatamente consideradas diferentes. Assim, evita-se a criação dos Workflows Influenciais e a realização dos demais cálculos para todos PMs dos Registros de Execução, evitando desperdício de tempo e processamento.

4.2. Workflow Influencial e Mapeamentos de Atividades

Após calcular a SP do par de atividades sendo analisado (a_1 e a_2), caso esta resulte em um valor maior que zero, é necessário avançar na solução calculando os Workflows Influenciais (W_1 e W_2) das atividades e fazendo o Mapeamento de Atividades similares nos dois *workflows*. O algoritmo que monta o Workflow Influencial a partir de uma dada atividade não é detalhado neste artigo por limitação de espaço, porém seu funcionamento é bastante simples. Baseado na definição de Workflow Influencial (Seção 3.3), dada uma atividade a, basta extrair do *workflow* original a(s) atividade(s) que sigam as seguintes propriedades: (*i*) atividades que antecedem a, (*ii*) que estão em paralelo com a ou (*iii*) que seja a própria atividade a. As atividades que respeitam pelo menos uma das três propriedades são inseridas no Workflow Influencial na mesma ordem que aparecem no *workflow* original mantendo-se também as mesmas transições.

Uma vez calculados os Workflows Influenciais W_1 e W_2, procede-se então com o Mapeamento de Atividades similares nesses dois *workflows*. Tal mapeamento é necessário porque para o cálculo de similaridade de *workflows* é preciso comparar as atividades contidas em cada *workflow* par a par. Porém, não é possível determinar diretamente quais atividades são correspondentes nos *workflows* para formar os pares, uma vez que estas são objetos compostos de operação e participantes. Sendo assim o mapeamento é feito considerando as SP entre os pares de atividades.

Um Mapeamento de Atividades pode ser definido como $m = \langle a_1, a_2, sp \rangle$, no qual:

- a_1 é a atividade do primeiro *workflow*;
- a_2 é a atividade correspondente do segundo *workflow*;
- sp representa a Similaridade Pontual entre a_1 e a_2.

Sendo assim, pode-se criar um conjunto com todos os mapeamentos dos *workflows* W_1 e W_2 representado por $Maps(W_1, W_2)$ com a restrição de que as atividades pertencentes a esses mapeamentos não aparecem repetidamente. Em outras palavras, cada atividade de W_1 será mapeada em no máximo uma atividade de W_2, sendo que se não for encontrada uma atividade correspondente o mapeamento não é criado.

A partir disso, o Algoritmo 2 pode ser utilizado para capturar os mapeamentos entre as atividades de dois *workflows*. Conforme esse algoritmo, para obter os mapeamentos entre os Workflows Influenciais, pode-se construir duas pilhas: uma com as atividades de W_1 (Linha 2) e outra com as atividades de W_2 (Linha 7), em que a primeira atividade de cada *workflow* está na base da pilha. Ao retirar-se cada atividade da primeira pilha (Linha 11), retiram-se atividades da segunda a pilha (Linha 14) até que se tenha uma SP, entre estas, maior que zero. Assim, cada mapeamento é capturado e colocado num conjunto com todos os mapeamentos (Linha 21). Percebe-se que esse algoritmo possui uma complexidade de fator quadrático, já que num pior caso, todos os possíveis pares de atividades tem suas SPs calculadas.

Algoritmo 2 MAPS

Entradas: W_1, W_2 e um tipo de falha ft
Saídas: $Maps$ conjunto com mapeamentos $m = \langle a_1, a_2, sp \rangle$

1: $Maps \leftarrow \varnothing$
2: $P_1 \leftarrow novaPilha()$
3: **para cada** Atividade $a \in W_1$ */*partindo-se da atividade inicial*/* **faça**
4: $P_1.push(a)$
5: **fim para**
6: $P_2 \leftarrow novaPilha()$
7: **para cada** Atividade $a \in W_2$ */*partindo-se da atividade inicial*/* **faça**
8: $P_2.push(a)$
9: **fim para**
10: **enquanto** $P_1.naoVazio()$ **faça**
11: $a_1 \leftarrow P_1.pop()$
12: $L \leftarrow \varnothing$
13: **repita**
14: $a_2 \leftarrow P_2.pop()$
15: $sp \leftarrow SP(a_1, a_2, ft)$
16: **se** $sp = 0$ **então**
17: $L \leftarrow L \cup \{a_2\}$
18: **fim se**
19: **enquanto** $sp = 0$ **E** $P_2.naoVazio()$
20: **se** $sp > 0$ **então**
21: $Maps \leftarrow Maps \cup \{\langle a_1, a_2, sp \rangle\}$
22: **fim se**
23: **para cada** $a_2 \in L$ **faça**
24: $P_2.push(a_2)$
25: **fim para**
26: **fim enquanto**
27: **retorna** $Maps$

4.3. Similaridade de Workflows

Para obter a similaridade entre dois *workflows*, parte-se de definições de similaridade de outros autores que usam o conceito de distância para calcular a similaridade entre duas entidades [Li *et al.* 2008]. Essa distância é a soma de operações de inserção, remoção e substituição necessárias para transformar uma entidade noutra. Considerando o conceito de distância é possível derivar a seguinte equação para calcular a similaridade entre dois conjuntos A e B: $sim(A, B) = 1 - \frac{ins+rem+sub}{|A \cup B|}$. Sabendo que $ins + rem = |A \cup B| - |A \cap B|$, ou seja, que o número de inserções e remoções é igual ao número de atividades diferentes, pode-se derivar a seguinte equação: $sim(A, B) = \frac{|A \cap B| - sub}{|A \cup B|}$.

Seguindo esse raciocínio, pode-se usar conceito de Similaridade Pontual, realizando uma soma dos valores de sp dos mapeamentos ao invés do cardinal da intersecção dos conjuntos. Além disso, pode-se interpretar $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$, onde $|A_1 \cap A_2| = |Maps(W_1, W_2)|$, ou seja, pela soma do número de atividades contidas nos *workflows* subtraída pelo número de mapeamentos. Assim, para calcular o escore de simi-

laridade de *workflows* utiliza-se neste trabalho a Equação 2, onde A_1 e A_2 são conjuntos não ordenados que contém as atividades de W_1 e W_2 respectivamente.

$$SW_{(W_1,W_2)} = \frac{\sum_{m \in Maps} sp_m - subst(W_1, W_2)}{|A_1| + |A_2| - |Maps(W_1, W_2)|} \quad (2)$$

Para o cálculo do número de substituições necessário na Equação 2, utiliza-se a solução proposta por Li em [Li *et al.* 2008], em que a partir das atividades coincidentes em ambos *workflows* busca-se, através da lógica digital, encontrar o menor número de troca de posições (substituições) entre as atividades. Para isso, a partir do conjunto de atividades comum aos *workflows* montam-se matrizes com informações sobre a ordem de execução das atividades para cada *workflow*. A seguir, extrai-se uma expressão lógica com os conflitos encontrados a partir dessas duas matrizes. Com tamanho do maior termo, obtido a partir da minimização dessa expressão lógica, obtém-se o número de substituições.

Para calcular a distância de substituições para similaridade entre PMs, ao invés de utilizar as atividades comuns dos *workflows*, utilizam-se os mapeamentos obtidos, já que com estes é possível obter as atividades correspondentes nos *workflows*. Assim duas matrizes de ordenação são geradas, uma relativa a posição da primeira atividade dos mapeamentos e outra a partir da segunda. Após obter-se a expressão minimizada a partir dos conflitos das matrizes de ordenação dos mapeamentos, cada termo será valorado com a soma das Similaridades Pontuais dos mapeamentos que devem ser reposicionados.

4.4. Similaridade Combinada

Compondo os escores de Similaridade Pontual (SP) entre as atividades analisadas e de Similaridade de Workflows (SW) entre os Workflows Influenciais dessas atividades obtém-se o valor chamado neste trabalho de Similaridade de Combinada (SC), conforme a Equação 3.

$$SC_{(a_1,a_2)} = SP_{(a_1,a_2)} \cdot SW_{(infl(a_1),infl(a_2))} \quad (3)$$

Os valores obtidos para SC das atividades analisadas são organizados em um Relatório de Similaridade que é utilizado no cálculo de risco das atividades do Plano de Mudança analisado. As probabilidades de falha calculadas por uma solução de estimativa de riscos para as atividades extraídas dos Registros de Execução podem ser então ponderadas pelos valores de SC. Desse modo, mais peso é atribuído às probabilidades das atividades mais similares, permitindo a utilização adequada dos históricos de execução de PMs similares. Além disso, convém também salientar, que por tratar-se de um cálculo de escore de similaridade podem surgir falsos negativos que podem comprometer a análise de risco. Para amenizar esse problema, seria interessante estabelecer, por exemplo, um *threshold* de similaridade para inibir a inserção de ruído na análise causada por atividades com similaridade muito baixa.

5. Estudo de Caso

Para avaliação da eficácia da solução, propomos um estudo de caso, em que uma empresa de *hosting* oferece o serviço de instalação, configuração e hospedagem de servidores de

webmail utilizando a plataforma *Horde*. Seguindo as boas práticas, recomendadas pelo ITIL, RFCs para diferentes máquinas são especificadas conforme requistos de configuração especificados pelos clientes. Os PMs gerados a partir dessas RFCs estão representados na Figura 2. Todas essas RFCs possuem a instalação de um sistema operacional Linux - Fedora ou Debian -, a instalação e configuração de Apache e PHP, e a instalação e configuração do *Horde Webmail*. Além disso, algumas RFCs também fazem a instalação de banco de dados MySQL, outras de PostgreSQL, e ainda outras utilizam o banco de dados já instalado em alguma outra máquina, para fornecer o armazenamento ao serviço de *webmail*. Também, certas atividades variam de posição entre diferentes RFCs. Algumas dessas atividades são executadas manualmente (destacadas com hachuras na Figura 2), tais são a instalação do sistema operacional e configuração do *Horde Webmail*, sendo que um mesmo perfil de humano está associado a estas.

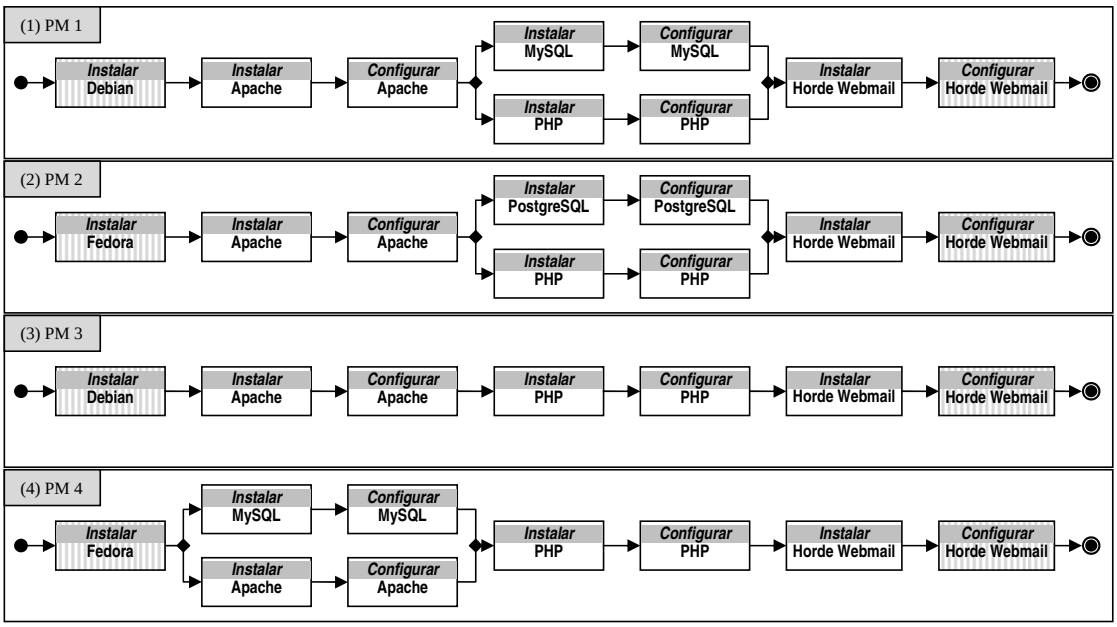


Figura 2. Planos de Mudança do Estudo de Caso

5.1. Análise das Similaridades

Observando-se a atividade de instalação da *Horde Webmail* do PM 4 e verificando a sua SC para Falhas de Atividade (FA) em relação as demais atividades desses PMs, nota-se que apenas as atividades *Instalar Horde Webmail* nos PMs têm SP maior que zero, já que são as únicas que possuem operação (*Instalar*) e participante de *software* (*Horde Webmail*) idênticos. Considerando essa atividade nos quatro PMs, a partir dos Workflows Influenciais obtidos com essas atividades - os quais são os próprios *workflows* excetuando-se a atividade *Configurar Horde Webmail* - obtém-se os mapeamentos apresentados na Tabela 1. Nessa tabela, estão apresentadas, por simplicidade, apenas a operação, participante de *software* e SPs em relação a essas atividades nos diferentes PMs.

Nesses mapeamentos, nota-se que as atividades *Instalar Fedora*, a qual possui um humano em comum com a mesma atividade do PM 4 apresenta SP de $0,50$, já que num total de quatro participantes apresenta dois em comum e dois distintos (*hardware*). Já as demais atividades, algumas não possuem mapeamentos, outras possuem SP de $0,33$, pois apenas o participante de *software* é idêntico, diferindo em 2 participantes de *hardware*.

Tabela 1. Mapeamentos das Atividades

	PM 1	PM 2	PM 3	PM 4
Instalar Fedora	-	0,50	-	1,00
Instalar Apache	0,33	0,33	0,33	1,00
Configurar Apache	0,33	0,33	0,33	1,00
Instalar MySQL	0,33	-	-	1,00
Configurar MySQL	0,33	-	-	1,00
Instalar PHP	0,33	0,33	0,33	1,00
Configurar PHP	0,33	0,33	0,33	1,00
Instalar Horde Webmail	0,33	0,33	0,33	1,00
Distância de Substituição	0,67	0,00	0,00	0,00
Soma das Similariades Pontuais	2,33	2,17	1,67	8,00
Tamanho Mapeamentos	7	6	5	8
Similaridade de Workflow	0,19	0,22	0,19	1,00
Similaridade Combinada	0,06	0,07	0,06	1,00

Além disso, na parte inferior da tabela, tem-se a soma dos mapeamentos e o número de mapeamentos, a serem usados para calcular a Similaridade de Workflow.

Através dos mapeamentos, pode ser feito o cálculo de distância de substituição, no qual verifica-se que apenas entre PMs 1 e 4 nas atividades *Instalar* e *Configurar MySQL* há conflitos de posição, entre estes obteve-se a distância de substituição no valor de $0,66$, ou seja, a soma das SP dessas atividades. A partir dos dados apresentados na tabela, podemos aplicar a Equação 2, de Similaridade de Workflow, obtendo os escores apresentados na mesma tabela. Para chegar ao escore final de SC, multiplicamos os escores de Similaridade de Workflow e Pontual da atividade analisada - *Instalar Horde Webmail* - seguindo a Equação 3.

5.2. Comparativo

Ao calcular-se as SCs de todas as atividades *Instalar Web Application* nos diferentes PMs, obtém-se os valores dispostos na mos a Tabela 2 (a). Para comparação, foram calculados os escores de similaridade para as mesmas atividades utilizando uma solução anterior proposta por Wickboldt *et. al* [Wickboldt *et al.* 2009b], cujos resultados encontram-se na Tabela 2 (b). Além disso, convém salientar que pelo fato de a similaridade ser comutativa, omite-se os valores da diagonal inferior da tabela.

Tabela 2. Matriz de Similaridades

(a)	(a) Similaridade Combinada				(b)	Similaridade anterior			
	PM 1	PM 2	PM 3	PM 4		PM 1	PM 2	PM 3	PM 4
PM 1	1,000	0,051	0,090	0,062	PM 1	1,000	0,313	0,396	0,438
PM 2		1,000	0,062	0,072	PM 2		1,000	0,313	0,396
PM 3			1,000	0,062	PM 3			1,000	0,313
PM 4				1,000	PM 4				1,000

Comparando-se os resultados obtidos com a métrica proposta por Wickboldt *et. al* aos resultados de Similaridade Combinada, percebe-se que o fato de esta nova métrica combinar os escores de Similaridade de Workflows e Pontual faz com que a similaridade

apresente valores menores em relação a solução anterior, uma vez que esta considerava apenas a similaridade da estrutura dos *workflows*. Isso é realmente interessante para a estimativa da probabilidade de falhas, pois quando se analisa riscos de PM que possuem seu próprio histórico de execução, as falhas desses planos terão muito mais peso do que as de outros planos apenas similares. Mesmo assim, os planos similares ainda possuem influência sobre o resultado final das probabilidades e, no caso de mudanças recém planejadas, serão determinantes para a obtenção dessa estimativa.Além disso, também verifica-se que pelo fato de a Similaridade Combinada levar em conta a posição das atividades no *workflow*, esta métrica apresenta um escore mais refinado em relação a solução anterior. Em certos casos isso pode alterar a ordem das atividades mais similares, como no caso em que na métrica anterior, PM 4 apresenta maior similaridade que PM 3 em relação a PM 1, já na nova métrica, ocorre a situação oposta.

6. Conclusão

Neste trabalho, foi proposta uma nova métrica para cômputo de similaridade de atividades de PMs visando aprimorar a análise de riscos baseada em dados históricos. Foi visto que nessa métrica de similaridade entre os principais aspectos levados em conta estão a importância de se considerar atividades que ocorrem antes da atividade analisada e a comparação dos participantes das atividades, relacionando-os aos seus tipos.

Os resultados obtidos a partir da execução de casos de testes numa infra-estrutura emulada, mostram a eficácia da solução em capturar os aspectos fundamentais de similaridade. Também a partir da comparação com solução anterior foi possível verificar que os escores obtidos apresentam uma maior amplitude, o qual reflete melhor as diferenças entre as atividades e torna a estimativa de probabilidade de falhas mais precisa.

Em trabalhos futuros, pretende-se ampliar os aspectos abordados, intrínsecos às características das infra-estruturas, refinando o conceito de Workflow Influencial. Além disso, pode-se estender a aplicabilidade da solução para outros contextos relacionadas como refinamento e alinhamento de planos, estimativa de custos e tempo, sempre aproveitando a base de informações históricas. A solução também pode ser usada numa abordagem evolutiva de infra-estruturas de TI, em que a partir de dados e decisões passadas, o sistema auxiliaria na tomada de decisões futuras.

O presente artigo foi alcançado em cooperação com a *Hewlett-Packard Brasil Ltda.* e com recursos provenientes da Lei de Informática (Lei nº 8.248, de 1991).

Referências

Chartrand, G., Kubicki, G., e Schultz, M. (1998). Graph similarity and distance in graphs. *Aequationes Mathematicae*, 55(1):129–145.

Cohen, W., Ravikumar, P., e Fienberg, S. (2003). A comparison of string distance metrics for name-matching tasks. Em *IJCAI-2003 Workshop on Information Integration on the Web (IIWeb-03)*, páginas 9–10.

Cordeiro, W. L. C., Machado, G. S., Daitx, F. F., *et al.* (2008). A Template-based Solution to Support Knowledge Reuse in IT Change Design. Em *11th IEEE/IFIP Network Operations and Management Symposium (NOMS 2008)*, páginas 355–362.

Hidders, J., Dumas, M., van der Aalst, W., ter Hofstede, A., e Verelst, J. (2005). When are two workflows the same? Em *Proceedings of the 2005 Australasian symposium on Theory of computing-Volume 41*, página 11. Australian Computer Society, Inc.

ITIL (2007). ITIL - Information Technology Infrastructure Library: Service Transition Version 3.0. Office of Government Commerce (OGC).

ITIL (2009). ITIL - Information Technology Infrastructure Library. Office of Government Commerce (OGC). Disponível em: http://www.itil-officialsite.com/. Acessado em: out. 2009.

Levenshtein, V. (1966). Binary codes capable of correcting deletions, insertions, and reversals. Em *Soviet Physics-Doklady*, volume 10.

Li, C., Reichert, M., e Wombacher, A. (2008). On measuring process model similarity based on high-level change operations. Em *27th International Conference on Conceptual Modeling (ER 2008)*, páginas 248–264.

Monge, A. e Elkan, C. (1996). The field matching problem: Algorithms and applications. Em *Second International Conference on Knowledge Discovery and Data Mining (KDD 96)*, páginas 267–270.

Office of Government Commerce (2007). Management of risk: Guidance for practitioners. Office of Government Commerce (OGC).

Sauvé, J., Santos, R. A., Almeida, R. R., Moura, A., *et al.* (2007). On the Risk Exposure and Priority Determination of Changes in IT Service Management. Em *18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2007)*, páginas 147–158.

Setzer, T., Bhattacharya, K., e Ludwig, H. (2008). Decision support for service transition management Enforce change scheduling by performing change risk and business impact analysis. Em *11th IEEE/IFIP Network Operations and Management Symposium (NOMS 2008)*, páginas 200–207.

Van der Aalst, W. e Basten, T. (2002). Inheritance of workflows: an approach to tackling problems related to change. *Theoretical Computer Science*, 270(1-2):125–203.

Van der Aalst, W., de Medeiros, A., e Weijters, A. (2006). Process Equivalence: Comparing Two Process Models Based on Observed Behavior. Em *4th International Conference on Business Process Management (BPM 2006)*, volume 4102, páginas 129–144.

Van Dongen, B., Dijkman, R., e Mendling, J. (2008). Measuring similarity between business process models. Em *CAiSE*, páginas 450–464. Springer.

Wickboldt, J., Lunardi, R., Machado, G., *et al.* (2009a). Automatizando a Estimativa de Riscos em Sistemas de Gerenciamento de Mudanças em TI. Em *XXVII Simpósio Brasileiro de Redes de Computadores (SBRC 2009)*, páginas 423–436.

Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., *et al.* (2009b). Improving IT Change Management Processes with Automated Risk Assessment. Em *20th IFIP/IEEE International Workshop on Distributed System: Operations and Management (DSOM 2009)*, páginas 71–84.

Wickboldt, J. A., Machado, G. S., Cordeiro, W. L. C., *et al.* (2009c). A Solution to Support Risk Analysis on IT Change Management. Em *11th IFIP/IEEE International Symposim on Integrated Network Management (IM 2009)*, páginas 445–452.

Wombacher, A. e Rozie, M. (2006). Evaluation of workflow similarity measures in service discovery. *Service Oriented Electronic Commerce*, 7:26.

Using a Cloud-based Event Service for Managing Context Information in Mobile and Ubiquitous Systems

Waldir R. Pires Junior[1], Antonio A. F. Loureiro[1], Ricardo A. R. Oliveira[2]

[1]Department of Computer Science – Federal University of Minas Gerais
Belo Horizonte – MG – Brazil

[2]Department of Computer Science – Federal University of Ouro Preto
Ouro Preto – MG – Brazil.

{wpjr,loureiro}@dcc.ufmg.br, rabelo@iceb.ufop.br

Abstract. *In mobile and ubiquitous computing systems, profile and context information from mobile users constantly change over a period of time. It is also desired for local and remote services to effortlessly access this information for adaptation of activities and event notification for mobile users. This work proposes an event-based system for managing context information in ubiquitous services and applications. This approach uses an event service to manage the events representing local and remote changes in the environment, allowing relevant information to be shared amongst interested services and mobile users. In our tests, an event service (tourist guide scenario) proved useful in disseminating changes in profile and context information between entities in a simulated ubiquitous environment.*

Resumo. *Em sistemas computacionais móveis e ubiquos, informações de perfil e contexto de usuário móveis podem sofrer mudanças constantes durante um determinado período de tempo. É desejável também que serviços locais e remotos possam acessar de uma forma simples e unificada estas informações a fim de proverem recursos tais como adaptação de atividades e notificação de eventos para usuários móveis. Este trabalho propõe um sistema baseado em eventos para o gerenciamento de mudanças de perfil e contexto locais e remotos, permitindo assim o compartilhamento de informações entre serviços e usuários móveis de interesse. Nos testes realizados (guia turístico), o servidor de eventos proposto mostrou-se útil em disseminar as mudanças de informações de perfil e contexto entre entidades em um ambiente ubíquo simulado.*

1. Introduction

Ubiquitous computing defines a new computational model of human-machine interaction in which information processing is integrated to daily objects and activities for the user. In this new paradigm, a user can activate and participate in several simultaneous and unconscious tasks and activities, in some cases not even being aware of the devices present in the surrounding environment. This introduces the necessity of context-aware computing, which proposes the capability of devices to sense changes in the environment and in the user's behavior. Context is defined [Dey 2001] as being "any information that can be used to characterize the situation of entities", such as the location, time of day, people, devices and services nearby, and user activities. Ubiquitous computing makes use of this

information collected from the environment for context definition and service adaptation in real time. This adaptation is defined [Rossi and Tari 2006] as the capacity of a system or middleware of modifying its behavior in response to changes in the environmental context. In this way, mobile applications as well as remote services can utilize the information collected and present at the context for providing services and content for the mobile user and for applications and services present at the mobile device.

Ubiquitous environments, in general, contain applications and network elements that are both heterogeneous and distributed in fashion. They are heterogeneous in the sense of performing different types of tasks for the user, requiring different sets of hardware and software components. They are also distributed in such a way that services may be composed of more than one computing element. For instance, a network element may depend on other devices for obtaining information about the environment and executing tasks for the user. As a result, a distributed communication model is required to seamlessly integrate these elements in the environment.

In the following, we briefly describe a tourist guide application that conveys the ideas discussed in this work. Suppose a tourist begins his/her day at the hotel and uses a mobile phone or PDA to search for tourist attractions and confirming the purchase of electronic tickets. While the tourist guides (people and companies) are contacted by the guiding system, the tourist can confirm the weather forecast and elaborate a route around the city. The route information is sent to the system, which offers existing services in the path such as shopping options, restaurants, among other activities.

After the tourist has begun his/her trip, the tourist guide application, based on previous defined interests and the necessary tickets purchased early in the morning, presents some leisure options that interest him/her the most. Caring about good services, the tourist remembers to leave a favorable comment to this guide in the service quality evaluation system. While visiting each attraction point, the tourist receives at his/her mobile device an electronic flyer describing the attraction and, according to his/her interests, some propaganda of products on sale at each location.

At any moment, the tourist may change his/her path. The guiding system running on the mobile device detects this change in the location and updates the information related to the services offered in this new path. In case the tourist is lost, the user can request some directions from the map service provided by the system, allowing him/her to return to the previously planned route and the attractions defined previously, or follow onto a new attraction of interest.

1.1. Problem and Contribution

Depending on the scenarios involved, user profile and context information may suffer constant changes over a period of time. Take for instance, changes of weather and traffic information, user or device location and state. Tourist guide applications are a good scenario example, since they contain virtually all the characteristics mentioned above. Activities initially selected by the user may become unfeasible due to traffic and/or weather conditions at that region or the user may simply not feel well or up to performing that activity due to his/her condition. The mobile device may also suffer difficulties or limitations at a certain moment, such as energy constraints, connectivity state and transmission costs.

This variability in profile and context information at context-aware ubiquitous applications promotes a significant challenge in managing these changes in a distributed mobile computing environment. This challenge includes the need to detect, collect, process, publish, subscribe and consume occurring events in the system. These changes occur in the environment (e.g., physical or logical) where the device is located, and the events generated must incorporate information relative to these changes. Physical context can be defined as the information relative to the outside environment, such as the user location, traffic and weather states, among others. Logical context relates to the conditions concerning the user and the mobile device, such as mood, time availability, battery level, connectivity state, among others. Interested event consumers use this information for reaction to changes detected, for example, by the means of adaptation and notification.

The main contributions of this work are:

- **Management of local/remote profile and context information from the user**: This work provides the provisioning of profile and context information from the user, application and the environment to other entities (e.g., other mobile users and Web-based services) in a mobile/ubiquitous system.
- **Fast provisioning of profile and context information from the user to other entities**: This work allows ubiquitous applications and services to distribute, access and share profile and context information amongst other entities in a decoupled and distributed manner by using event objects and notification messages sent over the wireless network.
- **Usage of a cloud-based infrastructure for the provisioning of ubiquitous applications and services**: This work makes use of cloud computing model based on some features such as the virtualization of hardware and software resources at the server side, making these features accessible in a seamless manner in the form of services on the Internet.

This paper is organized as follows. In Section 2, we briefly describe the related work. In Section 3, we present the event-based model proposed in this work, its architecture and the event processing workflow. In Section 4, we present the case study chosen for evaluating the proposed service called the DroidGuide. In Section 5, we discuss the conclusions and future work.

2. Related Work

Context-aware computing in ubiquitous environments and event-based distributed systems define the main areas of research of our work. The event-based communication model defined in Meier and Cahill [Meier and Cahill 2002] describes a useful paradigm in providing the interconnection between elements that comprise applications for ubiquitous environments in an asynchronous manner. This model allows the association between application components (producers and consumers) and events that are generated in ubiquitous system by the means of notification messages. It enables elements (devices, components and applications) to react to state changes of other elements, providing interested parties with notification messages based on these changes.

Muhl et al. [Muhl et al. 2006] define an event as being an occurrence of interest that can be observed by a computer element (e.g., PC, sensor, or any other device). One can define an event in a more global aspect as being a change of state where a system

entity is responsible for creating an event instance representing the changes in which other elements will respond, react and/or adapt by the means of imposed rules at the service and application levels. In our work, changes in the environment are represented by event objects that may be consumed by client peers and Web services.

Caporuscio and Inverardi [Caporuscio and Inverardi 2005] present a design of an event-based system, which allows applications to detect events at a certain region and evaluate their relevance and uncertainty taking into account the applications' main context. This allows the application to adapt to certain environmental conditions and reach its purposes. A specification is presented which includes the design of a prototype based on a publish/subscribe middleware. Other event-based systems proposed include Sacramento et al. [Sacramento et al. 2004] who proposed a middleware architecture for the development of context-aware services and applications for wireless network environments. Carzaniga et al. [Carzaniga et al. 2001] also propose four architectural solutions for distributed event-based systems: client/server, acyclical P2P (Peer-to-Peer), redundant P2P and hybrid. Those proposals can be used in the construction of context-aware ubiquitous systems for the dissemination of context information amongst various client peers.

Despite the solutions above, we chose to utilize a client/server architecture provided by the cloud-based computing model for several reasons. Some justifications in using this model for the virtualization of services and resources over the Internet include support for popular Web-based application layer protocols such as HTTP and XMPP, service mobility (e.g., device and location independent), flexibility (e.g., speed in redefining computing resources and scalability) and the possibility for application designers to focus on other application issues rather than in service and platform infrastructure.

Several use case scenarios may benefit from the usage of ubiquitous applications and services. These scenarios in general contain functional requirements such as the need for collecting, processing and sharing profile and context information from the user/application, adaptation, and non-functional requirements such as security, usability and mobility. The adaptation occurs according to the user's intentions and interests, to the graphical interface and to available services for the mobile user while security involves privacy, authentication, authorization and anonymity. From all those scenarios, we chose to construct and evaluate one: an electronic tourist guide.

3. The Event-based Service

The service proposed in this work is based on the event-based model described in [Muhl et al. 2006]. Our model comprises of nodes in three different categories: client, server, and service. Client nodes represent the mobile users containing devices capable of accessing services over a wireless network. The server node contains an interface for accessing available information-based remote services. These services are represented by service nodes that can receive events from the client and server nodes and respond back to the server when required. Client nodes can access the available Web services and other client peers by using the existing server node.

An overview of the related scenario can be seen in Figure 1. In this overview, one can note the presence of mobile and fixed users accessing and providing information to services available over the Web. The information shared is represented by event objects created, published and consumed by each entity in the system. In order for entities to be

capable of publishing and consuming these events to all interested parties, an event-based server receives and dispatches events to consumers according to subscriptions to elements such as interested services, activities and topics. In this way, only events that match the entities interests are delivered to each client. This event-based service offers subscription and event management services related to profile and context information collected from participating entities in the system.

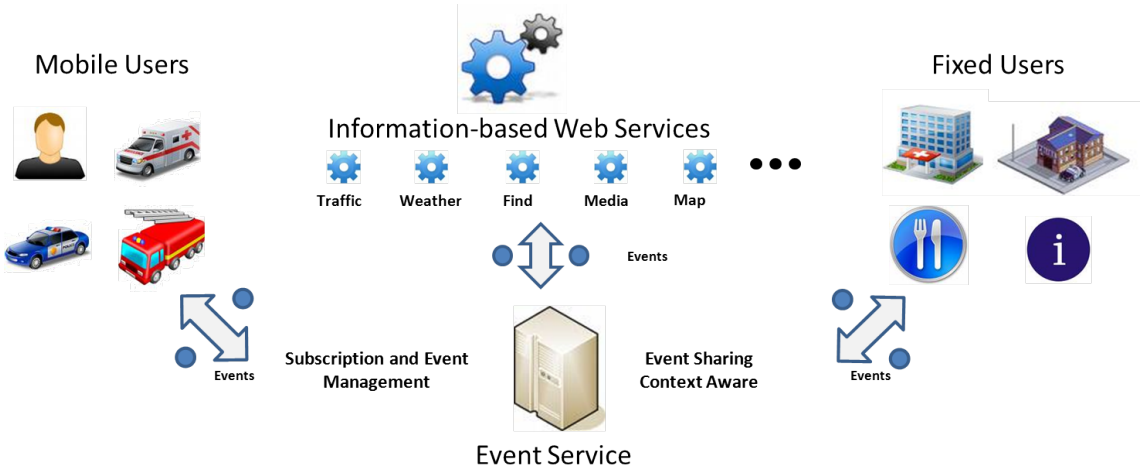


Figure 1. An overview of the proposed service.

The proposed service in our work contains several responsibilities in the ubiquitous computing environment. First, the service must periodically detect and collect changes in profile and context information from the mobile user. This is done in order to detect explicit and implicit changes in the environment, such as changes in location, interests and conditions, among others. In order to maximize the communication between client and server peers, the event processor located at the client plays an important role by creating event objects whenever there are local changes in profile and context information. In this way, the processor only reports the collected changes to the remote event service located at the server.

Secondly, our event service allows access to profile and context information by Web-based services in the form of event subscriptions based on interest topics. Suppose, for instance, that the mobile user wishes to change his logical context condition, such as mood or hunger state. If the mobile user feels agitated or hungry, he/she updates this condition at the mobile application in execution while in transit or inside a tourist activity. With this logical context update, the event processor detects the changes and sends them to the event server for further processing. The event server then publishes this information to services interested in the user's mood and hunger states. Based on the information received, nearby services and activities can be offered to the user, allowing him/her to rest or eat in locations nearby his/her position. By defining his/her preferences, the mobile user informs the event server the desire to share his/her profile and context information, allowing these services to monitor and react to changes informed by the user.

3.1. System Architecture

The event-based service proposed in this work is composed of two main components: the event server residing at a remote Web server and the event processor located at the

client side. Both components are responsible for generating event objects representing changes in the user profile and context information. The event server is responsible for handling events generated at the server side and also process events detected at the client side by the event processor. In turn, the event processor manages events detected at the client side and receives notification messages from the event server. Web-based services can take advantage of the relevant local and remote context information collected by the event processor/service, by receiving and processing these events. As a result, the Event Service Module provides subscription, filtering and event notification services to mobile applications and services that are both local and remote in relation to the mobile user.

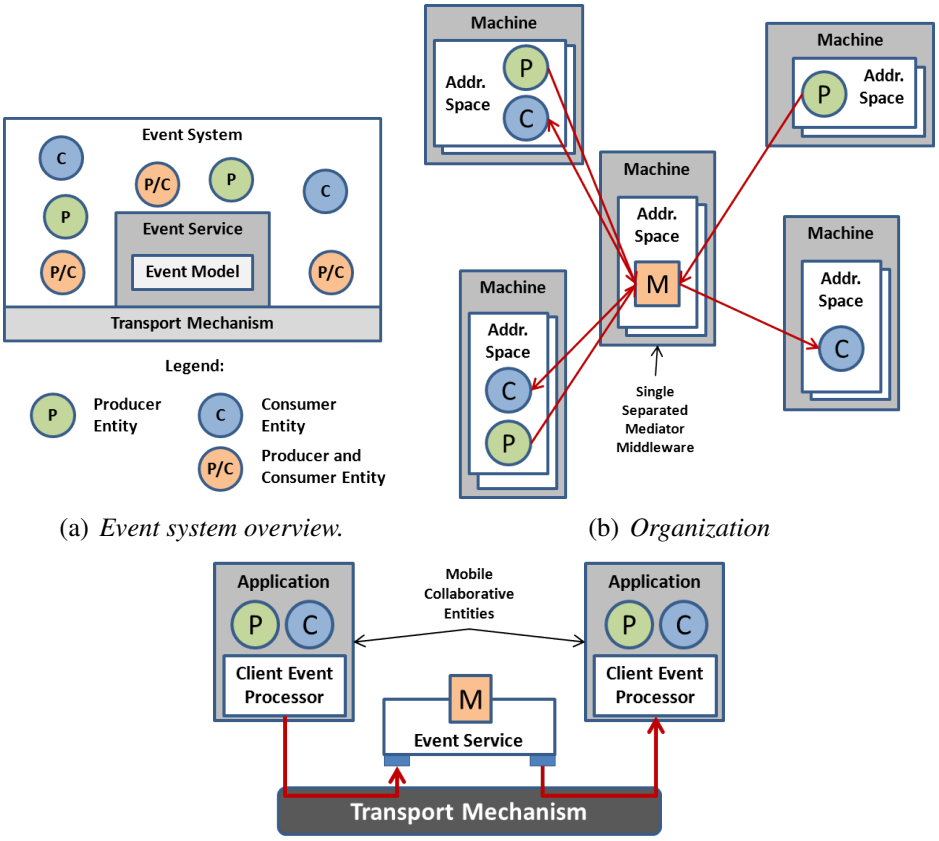
Different from the proposed architectures described in Carzaniga et al. [Carzaniga et al. 2001], our system uses a cloud-based solution where client peers connect to a unique server. This was done to simplify the development process and infrastructure provisioning at the server side. Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided in the form of a service on the Internet [Miller] . As a result, applications and infrastructure reside not locally, but at a remote location accessible over the Internet. Therefore, users do not require having the knowledge of, expertise in, or control over the technology infrastructure in the ”cloud” supporting them.

3.2. Event System Classification

A taxonomy has been proposed [Meier and Cahill 2002] for classification of event-based systems in several characteristics, such as the event model used, event service characteristics and functional/non-functional features available. Other event-based systems have been used in the classification, such as the CORBA notification service model[1], SIENA [Carzaniga et al. 2001], SECO [Haahr et al. 2000] and Hermes [Pietzuch and Bacon 2002]. Figure 2 describes the event service organization and interaction model as defined in the taxonomy for the service proposed in this work.

According to this taxonomy, the event service proposed in this work can be classified as follows. It implements a single mediator with a separated middleware, single centralized intermediate event model. It uses a single mediator between existing entities in the system, with this mediator being centralized and separated physically (different machines) and logically (different address space) from producers and consumers. In respect to the event propagation models defined in the taxonomy, our event system uses periodic pull, with typed events based on application specific attributes and without event hierarchy. The event service is an intermediate between mobile collaborative entities that are both producers and consumers. Events are delivered on a best-effort basis with no support for priority. Regarding failure handling, our system is characterized as a partial system failure for entities, functional partial system failure or total system failure for the event service middleware and partial or total system failure for the network. Other non-functional requirements such as security and ordering were omitted in our work. Tables 1 and 2 present the functional and non-functional features of the event service proposed in this work.

[1]http://www.omg.org/cgi-bin/doc?formal/04-10-13.pdf



(a) *Event system overview.* (b) *Organization*

(c) *Interaction model*

Figure 2. The organization and interaction model of the system proposed according to the taxonomy [Meier and Cahill 2002].

4. Case Study: DroidGuide

This section presents the first case scenario with the prototype implementation of the Tourist Guide scenario in the form of an emulated mobile application. This aims to evaluate the capacity of the mobile device to detect and collect profile and context information and allow user activity selection based on the profile information defined by the tourist.

The mobile application proposed provides several features to the mobile tourist user. First, it displays a map containing all the activities available for him/her to consume, as shown in Figure 3(a). Mobile users define their tourist profile data in order for the system to propose activities and provide information regarding interest topics, as shown in Figure 3(b). Mobile users also define their condition or state by entering their logical context, as shown in Figure 3(c). Once profile and context information is defined, the application may begin offering activities as well as notify mobile users regarding client and server based events.

The software platforms used in our prototype application were Google Android[2] and Google Web AppEngine[3] for the client and server, respectively. Communication was achieved by using HTTP request messages being sent from client to server while

[2]http://code.google.com/android/
[3]http://code.google.com/appengine/

Characteristic	Service Proposed	Description
Event model	Single mediator	One event service mediator between entities.
Event service organisation	separated single middleware	Event service middleware in different address space.
Event service interaction model and location	Single centralized intermediate	Entities interact with a single mediator.
Event propagation model	Periodic pull	Request-response communication.
Event type	Generic	Events are generic throughout the system.
Communication	Unicast, multicast and broadcast	Entities communicate with each other using published events.
Expressive power	Application specific attributes	Attributes defined for the event define its epression.
Type hierarchy support	No	Support for inheritance between events.
Event implementation	Object and String	Events are represented as objects at the serve side and Strings at the client side.
Event evaluation time	Propagation	Events are evaluated at propagation time.
Mobility	Collaborative entity	Mobile entities collaborate across the system space.

Table 1. Classification of the event service proposed in this work according to the taxonomy.

Characteristic	Service Proposed	Description
Support for composite events	Yes	Programatic support.
Event delivery	Best effort	No deadlines associated with events.
Event priority support	No	Priorities for events at the event queue.
Store occupancy	Configurable	Support for memory (hash table structure) or DBMS persistence.
Reliability	Reliable connection and (temporarily) and persistent	Usage of a connection-oriented protocol (HTTP/TCP/IP)
Security support	No	Authentication, authorization and criptography.
Entity failure	Partial system failure	Partial failure at the entity.
Middleware failure	Functional partial system failure or total system failure	Depending on the failure, it can be partial (recovery) or total (no recovery).
Network failure	Partial or total system failure	Depending on the entities at the communication, being partial (between entities) or total (between entities and middleware).

Table 2. Non-functional feature support according to the taxonomy.

the server communicates with clients via XML documents over the HTTP response messages. In our work, we used a pull-based [Muhl et al. 2006] client-server communication approach by sending periodic request messages from the client to the server. This enables the server to seamlessly send notification messages to client peers when required as well as the client peers to send data to the event service.

To simplify the implementation and integration of the many responsibilities that comprise the application, the DroidGuide guiding system was logically divided into modules with well defined responsibilities and relationships among them. As shown in Figure 4, these components are:

- At the mobile device: the profile and context management service (PCM), the client event processor (CEP) and the communication module (CM);
- At the server: the event processing service (EPS), the subscription manager (SM), the event container (EC) and the information-based remote-services container (IBWS).

From all modules, two of them should be noted due to their importance: the Client Event Processor (CEP) and the Communication Module (CM). The first one manages the

(a) Map with attractions. (b) User profile data. (c) User context data.

Figure 3. The Tourist Guide prototype developed on the Google Android Platform 2.0.

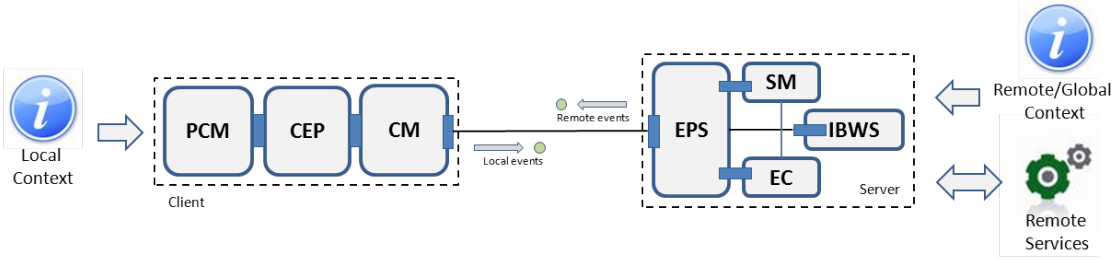


Figure 4. The Event-based system deployed into the DroidGuide application divided into modules.

changes in profile and context information by storing client events to be sent to the event server. The Communication Module manages the communication of all modules that make up the application, which include sending requests, receiving and processing XML messages from the server. The Event Processor uses a two-phase pull-based approach: (a) it sends HTTP GET requests from client to server, and (b) receives XML over HTTP response messages from the server to client. The communication module handles XML parsing of incoming data messages from the server, converting them to generic property-based objects. In our prototype, DOM (Document Object Model) parsing was used to convert XML messages to Java objects.

Located at the client side, the profile and context management service (PCM) is responsible for monitoring and collecting data regarding changes in profile and context information at the mobile device. This service submits the collected changes to the client event processor (CEP), which prepares the collected information for the communication module (CM). The communication module sends the information to the event process-

ing service (EPS) located at the server. Once the information arrives at the server, the event processing service creates event objects representing them, stores them at the event container (EC) and sends them to the corresponding consumers according to the existing subscriptions managed by the subscription manager (SM).

Once these consumers (e.g., remote services) receive the incoming events, they may also generate new events due either to the events received or changes in remote profile and context information. In this case, they also generate events that are sent to the event processing service. After storing the new events at the event container, the service requests the subscription manager for subscriptions related to the new events and generates notifications to be sent to the client. At the HTTP response message, the service sends the related notification messages to the client for further processing by the communication module and client event processor. This incoming message is presented to the mobile user, for example, in the form of a popup message alerting him of the event.

4.1. The Execution Flow

DroidGuide begins by requesting the tourist to login with his/her username and password. After the login process, the user is asked to define some attributes in his/her profile and context data, as shown in Figures 3(b) and 3(c). This can be later updated, even if in the future the tourist logs in again at another device containing the application. After the tourist defines his/her profile and context data, the event service takes action by monitoring local/individual or remote/global changes in this data. In the next step, the user is able to select available information-based remote services available at the remote data server for notification message provisioning. In our simulated scenario, two remote services were provided: traffic and weather.

After the tourist selects the interested services, the application begins selecting available tourist activities that can best suite his/her interests defined in the profile data, taking into account the six styles or interests already defined by the user: consumer, historical, environmental, gastronomical, bohemian, and cultural. The tourist grades each of these styles with a score from zero (not interested) to ten (totally interested). In general, every tourist activity available at the location contains a grade based on the same styles presented to the tourist. For instance, a restaurant activity has a high grade in the gastronomical style while a very low grade in environmental. Another activity, however, can have high grades in two or more styles such as in activities that relate to both historical and cultural styles. An example of the activity suggestion feature can be seen in Figure 5(b).

As proposed in the system, the tourist should also be capable of selecting other activities not initially presented to him/her by the system. The service capable of activity selection can be seen in Figure 5(b). For instance, there can be activities in which his/her friends have performed that were highly recommended to him/her and not initially suggested by the system. This is possible due to the publish/subscribe feature also available at the proposed event service. In our prototype, activity selection is treated in the same manner as in subscription to services and topics. Once the tourist selects the desired activities, he/she may begin visiting these activities.

During the execution process, the service can deliver notification messages to interested parties in case there are changes detected in the user's profile and context data.

(a) Remote services. (b) Tourist activities.

Figure 5. Subscription elements available to the mobile user.

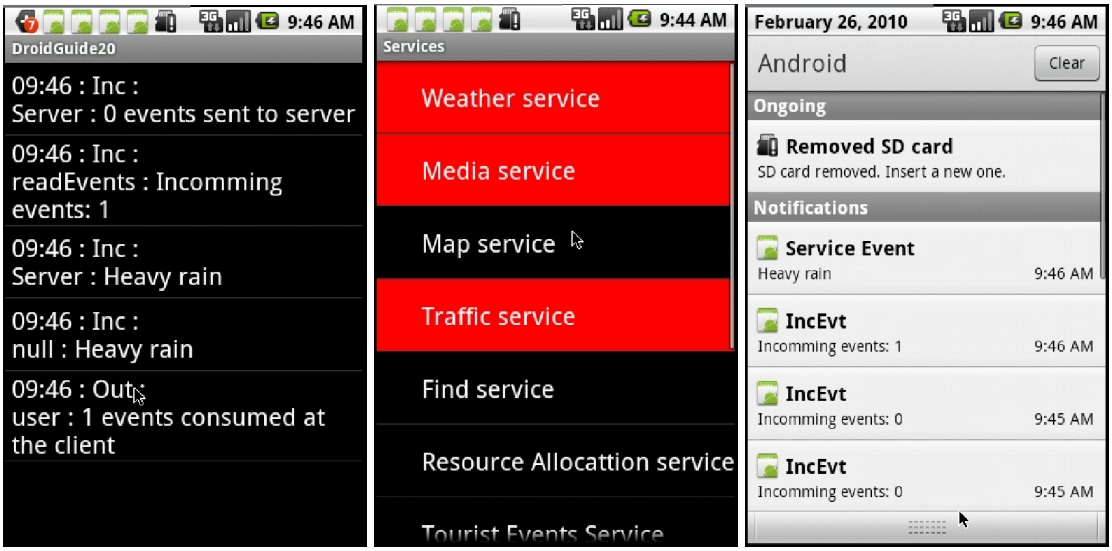
An example of a list of subscribed services can be seen in Figure 6(b). For instance, a remote restaurant finder service is interested in knowing when the tourist is hungry. When this occurs, the user updates his/her logical context data present at the mobile device. This change causes the event processor to send data to the server, allowing the creation of event objects representing the changes. The event service then shares these objects to interested/subscribed services. Once the information-based service receives the event object, it understands that a notification message must be sent to the user, informing him/her of a possible restaurant nearby. In the end, the user receives the notification informing him/her of the attraction nearby that can satisfy his/her hunger.

In our simulation, we created a weather event object at the server that was directly related to one of the tourist's interest topics and subscribed information-based remote services. Due to the subscription to the weather service, this service will notify the user with any changes of profile and context information occurring at the server – in our case a change in weather condition.

Figure 6 shows the creation of a server-side event and its notification at the client application. Figure 6(a) shows the notification screen presenting the incomming notification from the server. Figure 6(b) shows the list of remote services subscribed by the mobile user. Figure 6(c) shows the notification tab presenting the incomming notification to the user.

5. Conclusion and Future Work

In this work, we presented an event-based service for the management of local and remote profile and context information for client peers, as well as for information-based Web services. The event service was capable of capturing changes in profile and context data from both the client and the server sides. The events have been collected in the device and sent to the server by the communication module. According to the interests defined by the user in his/her profile, tourist activities were selected accordingly. Subscriptions



(a) Notification screen. (b) Subscribed services. (c) Notification tab.

Figure 6. Notification of a server side event at the client.

to information-based services showed the viability of using events in these services for ubiquitous applications. These services were capable of sending notification messages to the client application, due to the creation of remote event objects when changes in remote/global context information were detected.

The future work may follow in several directions: (i) the evaluation of the event-based service in other environments and scenarios (for instance, in vehicular networks and in elderly care centers), (ii) definition of event processing profiles allowing event processing configuration according to the needs of the application (e.g., client, client and server and server), (iii) security (user authentication, anonymity and authorization and data encryption/decryption of messages) and message compression during transmission, and (iv) the evaluation of collaborative context-aware computing scenarios, the relationship and interaction amongst client peers.

References

Caporuscio, M. and Inverardi, P. (2005). Uncertain event-based model for egocentric context sensing. In *SEM '05: Proceedings of the 5th international workshop on Software engineering and middleware*, pages 25–32, New York, NY, USA. ACM.

Carzaniga, A., Rosenblum, D. S., and Wolf, A. L. (2001). Design and evaluation of a wide-area event notification service. *ACM Trans. Comput. Syst.*, 19(3):332–383.

Dey, A. K. (2001). Understanding and using context. *Personal Ubiquitous Comput.*, 5(1):4–7.

Haahr, M., Meier, R., Nixon, P., Cahill, V., and Jul, E. (2000). Filtering and scalability in the eco distributed event model. In *PDSE '00: Proceedings of the International Symposium on Software Engineering for Parallel and Distributed Systems*, page 83, Washington, DC, USA. IEEE Computer Society.

Meier, R. and Cahill, V. (2002). Taxonomy of distributed event-based programming systems. In *ICDCSW '02: Proceedings of the 22nd International Conference on Distributed Computing Systems*, pages 585–588, Washington, DC, USA. IEEE Computer Society.

Miller, M. Cloud computing pros and cons for end users. http://www.informit.com/articles/article.aspx?p=1324280.

Muhl, G., Fiege, L., and Pietzuch, P. (2006). *Distributed Event-Based Systems*. Springer, 1st edition.

Pietzuch, P. R. and Bacon, J. (2002). Hermes: A distributed event-based middleware architecture. In *ICDCSW '02: Proceedings of the 22nd International Conference on Distributed Computing Systems*, pages 611–618, Washington, DC, USA. IEEE Computer Society.

Rossi, P. and Tari, Z. (2006). Software adaptation for service-oriented systems. In *MW4SOC '06: Proceedings of the 1st workshop on Middleware for Service Oriented Computing (MW4SOC 2006)*, pages 12–17, New York, NY, USA. ACM.

Sacramento, V., Endler, M., Rubinsztejn, H. K., Lima, L. S., Goncalves, K., Nascimento, F. N., and Bueno, G. A. (2004). Moca: A middleware for developing collaborative applications for mobile users. *IEEE Distributed Systems Online*, 5(10):2.

Filtro de Conteúdo para Sistemas SMS Baseado em Classificador Bayesiano e Agrupamento por Palavras

Dirceu Belém[1], Fátima Duarte-Figueiredo[1]

[1]Pontifícia Universidade Católica de Minas Gerais (PUC - Minas)
Rua Walter Ianni, 255, Belo Horizonte, Minas Gerais, 31980-110, MG
dirceu@fourtime.com, fatimafig@pucminas.br

Abstract. *There are many researches about e-mail spam filters. However, there are few researches that look at this issue for SMS (Short Message Service) systems. This is a result of the difficulty in having access to SMS platforms of mobile operators. Furthermore, the volume of spams to SMS systems has increased year after year. The main objective of this work is to propose the implementation of a content filter for SMS systems based on the Bayesian Classifier and word grouping. In order to evaluate the performance of this filter, 120 thousand messages sent from a content provider that services mobile operators were tested. The results demonstrated that the proposed filter reached a correct index spam detection close to 100%.*

Resumo. *Existem muitas pesquisas sobre filtro de spam para e-mails. No entanto, existem poucos trabalhos que abordam o assunto para sistemas SMS (Short Message Service). A quantidade de spams para sistemas SMS tem aumentado a cada ano. O principal objetivo deste trabalho é propor a implementação de um filtro de conteúdo para sistemas SMS baseado em classificador Bayesiano e agrupamento por palavras. Para avaliar o desempenho do filtro, foram utilizadas 120.000 mensagens de um provedor de conteúdo que presta serviço para operadoras de telefonia celular. Os resultados apresentados demonstraram que o filtro proposto obteve um índice de acerto na detecção de spams próximo de 100%.*

1. Introdução

Desde o lançamento da telefonia celular, até os dias de hoje, é possível perceber uma evolução dos dispositivos e dos serviços prestados pelas operadoras. Uma grande variedade de serviços passou a ser oferecida. O SMS (*Short Message Service*), conhecido popularmente como sistema de troca de mensagens de texto ou torpedos, tornou-se um dos mais importantes serviços, por ser de simples utilização e de baixo custo. A utilização dos serviços SMS representou, em 2007 12% da receita das operadoras de telefonia celular da Europa (Gartner, 2008). Na China, em 2000, foram enviadas um bilhão de mensagens SMS. Na Europa, em 2006, a receita das operadoras foi de 429,6 milhões de euros e aumentaria 30% em 2007, segundo He, Sun, Zheng, Wen (2008). As estimativas de faturamento global previstas até 2013, na utilização de serviços SMS, devem ser de US$ 177 milhões (Boas, 2008).

Considerando o alto percentual de mensagens indesejadas em sistemas SMS, este trabalho apresenta um filtro de conteúdo baseado em classificador Bayesiano, para

detectar spams previamente. Na bibliografia consultada, outros autores Deng e Peng (2006) implementaram filtros de conteúdo baseados em Classificadores Bayesianos. A proposta deste trabalho diferencia-se da deles por permitir o agrupamento de palavras das mensagens no filtro e na escalabilidade dos testes. O algoritmo desenvolvido na implementação do filtro, foi integrado a uma plataforma de envio de mensagens para sistemas SMS, de uma empresa provedora de conteúdo SMS, integrada a grandes operadoras de telefonia celular do país.

A implementação do filtro foi realizada em uma ESME (*External Short Message Entity*). Essa entidade é responsável por entregar as mensagens enviadas pelos provedores de conteúdo à SMSC (*Short Message Service Center*). Tanto a ESME quanto a SMSC são componentes de uma arquitetura da operadora de telefonia celular que será explicada detalhadamente no trabalho. O papel do filtro de conteúdo na ESME é classificar e bloquear as mensagens classificadas como spam.

Este trabalho está organizado da seguinte forma: a Seção 2 apresenta os principais conceitos, onde são apresentadas as tecnologias existentes sobre filtros de conteúdo. A Seção 3 apresenta os principais trabalhos relacionados. A Seção 4 apresenta a descrição do filtro baseado em Classificação Bayesiana e agrupamento por palavras. A Seção 5 apresenta os experimentos, os resultados e a análise. A Seção 6 apresenta as conclusões e os trabalhos futuros.

2. Principais Conceitos

2.1. Spam

Spam é definido por Sahami, Dumais, Heckerman e Horvitz (1998) como uma forma de bombardear caixas de mensagens com mensagens não solicitadas a respeito de tudo, desde artigos para venda e formas de como enriquecer rapidamente, a informações sobre como acessar sites pornográficos. Para Cranor e LaMacchia (1998), os principais fatores que contribuem para o crescimento do número de spam são a facilidade de enviá-lo para um grande número de destinatários e de se obter endereços de e-mails válidos, além do baixo custo de envio. Cormack e Lynam (2005), definem o spam como e-mail não solicitado, emitido de forma indiscriminada, direta ou indiretamente, por um remetente que não tem nenhum relacionamento com o destinatário. O spam pode ser considerado o equivalente eletrônico das correspondências indesejadas e dos telefonemas de telemarketing não solicitados.

2.2. Formas de Bloqueio e Detecção de Spam

As formas de bloqueio e detecção de um spam estão divididas em: listas de bloqueio, bloqueio temporário de mensagens (*greylisting*), autenticação da organização que está enviando aquele e-mail (*DomainKeys Identified Mail*) e filtros de conteúdo. As três primeiras técnicas se baseiam em bloquear o e-mail de acordo com o remetente ou quem está enviando o e-mail, podendo bloquear mensagens vindas de um remetente, servidor, ou domínio. A última técnica se baseia em analisar o conteúdo do e-mail e detectar se aquele e-mail é ou não spam. Algumas soluções podem utilizar mais de uma técnica ao mesmo tempo.

2.3. Filtros de Conteúdo propostos para E-mail

A filtragem de conteúdo consiste em analisar e identificar o conteúdo de acordo com uma classe, por exemplo, spam e não spam. Para que seja possível identificar as mensagens, o processo de filtragem precisa passar por um treinamento com uma amostra de mensagens das duas classes. Este processo de treinamento obtém os atributos necessários para a identificação e classificação das mensagens. Deng e Peng (2006), por exemplo, utilizam como atributos, quantidade de caracteres e o remetente, na identificação e classificação das mensagens spam e não spam.

Os primeiros filtros de conteúdo que surgiram foram para spams de e-mail, mas podem ser adaptados para sistemas SMS. Segundo Ming, Yunchun e Wei (2007), várias técnicas sobre filtragem de spam para e-mails foram criadas. Elas podem ser divididas em três técnicas: a primeira é baseada em palavra-chave, onde os algoritmos extraem características do corpo do e-mail e identifica as correspondências com essa palavra-chave. Essa técnica é considerada passiva e demorada. Por exemplo, quando os *spammers* alteram as palavras dos e-mails, o método se torna ineficaz por não encontrar as palavras e, quando há muitas palavras, as pesquisas são muito demoradas.

A segunda técnica filtra o conteúdo. Essa técnica pode ser vista como um caso particular de categorização de texto, onde apenas duas classes são possíveis: spam e não spam. As soluções que utilizam essa técnica estão entre os principais métodos: classificador Bayesiano, SVM (*Support Vector Machine*), K-NN (K-Vizinhos Mais Próximos), Redes Neurais Artificiais, Árvores *Boosting*, Aprendizado Baseado em Memória, Rocchio e Sistemas Imunológicos Artificiais. A filtragem de conteúdo possui algumas desvantagens. Primeiramente, ocorre um desperdício de largura de banda de rede, onde não é possível tomar decisão sobre o tipo do e-mail enquanto o mesmo não tenha sido baixado inteiramente no cliente. Em segundo lugar, é difícil garantir a atualidade da amostra, pela quantidade de e-mails e mudanças nos conteúdos de spam, sendo difícil garantir o efeito e a persistência do algoritmo anti-spam.

A terceira técnica é baseada na filtragem de spam. Essa técnica pode detectar spam e evitar as desvantagens da primeira e da segunda técnica. É uma técnica que reconhece spam através do comportamento dos usuários ao enviar novos e-mails, construindo o processo de decisão para receber e-mails. Essa técnica utiliza o comportamento dos *spammers* para detectar novos spams.

2.4. Classificador Bayesiano

A técnica filtragem de conteúdo baseada em classificador Bayesiano, segundo Silva (2009), é bastante utilizada em problemas de categorização de texto e em filtros anti-spam. A ideia básica é usar a probabilidade na estimativa de uma dada categoria presente em um documento ou texto. Assume-se que existe independência entre as palavras, tornando o filtro mais simples e rápido.

Na teoria da probabilidade, o teorema de Bayes é relacionado à probabilidade condicional de dois eventos aleatórios. Criado por Thomas Bayes, um famoso matemático britânico que viveu no século 18, o teorema de Bayes é utilizado para calcular probabilidades posteriores, a partir de informações coletadas no passado, e representa uma abordagem teórica estatística de inferência indutiva na resolução de problemas (Kantardzic 2003). Por exemplo, ao se observar alguns sintomas de um

paciente, é possível, utilizando-se o teorema, calcular a probabilidade de um diagnóstico (Sahami, Dumais, Heckerman e Horvitz, 1998).

De acordo com o teorema de Bayes, a probabilidade é dada por uma hipótese dos dados, considerada base posterior, que é proporcional ao produto da probabilidade vezes a probabilidade prévia. A probabilidade posterior representa o efeito dos dados atuais, enquanto a probabilidade prévia especifica a crença na hipótese, ou o que foi coletado anteriormente. O teorema nos permite combinar a probabilidade desses eventos independentes em um único resultado (Sahami, Dumais, Heckerman e Horvitz, 1998).

Kantardzic (2003) apresenta a classificação bayesiana da seguinte forma, seja X uma amostra de dados, cuja classe seja desconhecida, e seja H alguma hipótese, tal que os dados específicos da amostra X pertencem à classe C. Pode-se determinar $P(H \mid X)$, a probabilidade da hipótese H possui dados observados na amostra X, onde $P(H \mid X)$ é a probabilidade posterior que representa a confiança na hipótese. $P(H)$ é a probabilidade prévia de H, para qualquer amostra, independente de como a amostra dos dados aparecem. A probabilidade posterior $P(H \mid X)$ baseia-se em obter mais informações na probabilidade prévia $P(H)$. O teorema Bayesiano provê o cálculo da probabilidade posterior $P(H \mid X)$ utilizando as probabilidades $P(H)$, $P(X)$ e $P(X \mid H)$, conforme fórmula (1).

$$P(H \mid X) = \frac{P(X \mid H) \cdot P(H)}{P(X)} \qquad (1)$$

Suponha que existe um conjunto de m amostras $S = \{S_1, S_2, ..., S_m\}$ (conjunto de dados já treinados), onde cada amostra S_i é representada por um vetor de n dimensões $\{x_1, x_2, ..., x_n\}$. Valores de x_i correspondem aos atributos $A_1, A_2, ..., A_n$, respectivamente. Além disso, existem k classes $C_1, C_2, ..., C_k$ e todas as amostras pertence a uma dessas classes. Dada uma amostra de dados adicionais x (onde sua classe é desconhecida), é possível predizer a classe para x usando a probabilidade condicional mais elevada $P(C_i \mid X)$, onde $i = 1, ..., k$. As probabilidades são obtidas a partir do teorema de Bayes:

$$P(C_i \mid X) = \frac{P(X \mid C_i) \cdot P(C_i)}{P(X)} \qquad (2)$$

Em (2), $P(X)$ é constante para todas as classes, somente o produto $P(X \mid C_i) \cdot P(C_i)$ deve ser maximizado. $P(C_i)$ é o número de amostras treinadas para a classe C_i / m (m é o total de amostras treinadas). Tendo em vista a complexidade do cálculo de $P(X \mid C_i)$, especialmente para grandes conjuntos de dados, é realizado um pressuposto ingênuo de independência condicional entre os atributos. Utilizando esse pressuposto, é possível expressar $P(X \mid C_i)$ como um produto:

$$P(X \mid C_i) = \prod_{t=1}^{n} P(x_t \mid C_i) \qquad (3)$$

Em (3), x_t são valores para atributos na amostra X. As probabilidades $P(x_t \mid C_i)$ podem ser estimadas a partir do conjunto de dados treinados.

2.5. Filtros de Mensagens SMS

Dentre as técnicas conhecidas para filtragem de e-mail algumas delas também são utilizadas na filtragem de mensagens SMS. Listas de bloqueio e filtros de conteúdo, utilizando técnicas KNN, SVM e classificação Bayesiana, podem ser citados. Além dessas técnicas, foi encontrada também uma técnica chamada CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) nos trabalhos de He, Wen e Zheng (2008), Shahreza (2008), Zhang, He, Sun, Zheng e Wen (2008) e Shahreza (2006), onde é possível realizar um teste cognitivo para identificar um ser humano e um computador. Nesse caso, o filtro solicita uma resposta ao remetente sobre uma pergunta que não pode ser realizada por um sistema, inibindo, assim, as mensagens indevidas.

2.6. O problema do falso positivo e do falso negativo

Um dos erros inaceitáveis na detecção de spam é não enviar uma determinada mensagem ao usuário por classificá-la incorretamente como spam. Esse erro é denominado falso positivo. Ou seja, ao classificar essa mensagem, o algoritmo classifica essa mensagem como spam e não a envia ao usuário. Em programas de e-mail, esse problema pode ser parcialmente resolvido configurando-os para enviar mensagens classificadas como spam para uma pasta específica. Sendo assim, o usuário poderá verificar essa pasta em busca de mensagens não spam classificadas incorretamente. Um outro tipo de erro, denominado falso negativo, não é tão grave. O único aborrecimento é que o usuário vai receber novas mensagens spam em sua caixa de entrada de e-mails. Quando isso ocorrer, o único trabalho que o usuário terá será o de excluir essa mensagem, ou denunciá-la como spam, caso o seu programa de e-mails tenha essa opção (Assis, 2006).

3. Principais Trabalhos Relacionados

O trabalho apresentado por Deng e Peng (2006) propõe um filtro de spam baseado em classificador Bayesiano para sistemas SMS. A proposta de Deng e Peng (2006) foi combinar a solução do filtro com o atributo palavra, com o filtro com os atributos, telefone, URL, tamanho da mensagem, valores monetários, lista negra (*blacklist*) de remetentes a serem bloqueados e lista branca (*whitelist*) de remetentes confiáveis.

A conclusão apresentada por Deng e Peng (2006), no trabalho realizado, foi que, ao se adicionar novos atributos propostos no cálculo, os resultados apresentaram uma precisão maior para se classificar as mensagens como spam e não spam. Ou seja, o filtro com os novos atributos obteve um resultado superior quando se compara com o algoritmo sem os novos atributos, reduzindo o número de falsos positivos e falsos negativos. Os resultados obtidos por Deng e Peng (2006) para os testes realizados adicionando todos os atributos foi de 99,1% de acerto.

4. Descrição do filtro baseado em classificação Bayesiana e agrupamento por palavras

A proposta deste trabalho é a implementação de um filtro de conteúdo baseado em classificação Bayesiana para sistemas SMS. A classificação Bayesiana foi escolhida devido à facilidade de implementação e conforme mencionado anteriormente, o filtro implementado neste trabalho se difere dos propostos por outros autores por agrupar palavras no treinamento do filtro e por estar implementando dentro de uma ESME. Este trabalho propõe a utilização de apenas palavras e três atributos para a classificação dos filtros.

4.1. Implementação do Filtro

Resumidamente, o trabalho engloba processos descritos a seguir: foi desenvolvida uma ESME e implantada em uma operadora de telefonia celular. Essa ESME recebe as mensagens enviadas pelos provedores de conteúdo e classifica as mensagens como spam e não spam antes de enviar à SMSC da operadora de telefonia celular. Caso a mensagem seja classificada como não spam, essa mensagem será encaminhada a SMSC da operadora que enviará essa mensagem ao dispositivo móvel do usuário. Foi desenvolvido também um aplicativo em Java para os dispositivos que suportam o sistema operacional Android, onde o usuário poderá classificar as mensagens como spam ou não spam, contribuindo com a base de dados do filtro.

O filtro implementado trabalha sobre cada mensagem para classificá-la como spam ou não spam, da seguinte forma: retira-se os caracteres especiais, acentos, e stopwords, transforma-se todos os caracteres em minúsculos. O conjunto de palavras restantes é armazenado em um vetor. Esse vetor é percorrido sequencialmente, pegando uma, duas, três, quatro, ou cinco palavras, de acordo com a opção feita antes de se iniciar o filtro. Todas as combinações de uma a cinco palavras são armazenadas no vetor. Cada elemento do vetor pode ser consequentemente uma, duas, três, quatro ou cinco palavras. Além disso, cala elemento pode conter um valor agregado, ou seja, um atributo.

Inicialmente, foram obtidas 120.000 mensagens de uma ESME implantada em uma operadora de telefonia celular. As 120.000 mensagens foram classificadas manualmente como spam e não spam de acordo com o caso. Todas as palavras de cada mensagem foram listadas e agrupadas até no máximo cinco palavras. Foi estabelecida uma probabilidade de cada uma dessas palavras e grupos de palavras aparecerem em uma mensagem spam e não spam, através da fórmula de Bayes. Por exemplo, ao se receber uma mensagem com a palavra “compre” a maioria dos usuários consideraria essa mensagem como spam, e, raramente, encontraria essa palavra em uma mensagem considerada não spam. Por isso, foi necessário treinar o filtro para que fosse possível identificar a probabilidade de uma mensagem com a palavra “compre” spam. O mesmo foi realizado para o grupo de duas, três e quatro palavras, como por exemplo “compre agora”, “compre agora carro” e “compre agora carro imperdível”. Esse treino foi feito com 25.000 mensagens spam e 95.000 mensagens não spam, totalizando 1.405.285 grupos de uma a cinco palavras. Durante o treino, o filtro ajustou as probabilidades de cada uma das palavras e grupos encontrados nas mensagens, de acordo com a categoria, spam e não spam.

Foi realizada a remoção de *stopwords*, que consiste em descartar as palavras que pouco refletem o conteúdo de um documento ou são tão comuns que não distinguem nenhuma categoria dos documentos, como por exemplo, artigos e preposições. Cada idioma possui uma lista de palavras consideradas *stopwords*. A lista para o idioma português foi obtida em Balinski (Balinski 2002). Para Silva (2009), nem todas as palavras são igualmente significativas para representar uma categoria. Algumas carregam mais significado que outras. Normalmente, os substantivos, seguidos dos adjetivos e verbos carregam mais representatividade do que outras classes gramaticais como os pronomes, as conjunções e os artigos. A remoção das *stopwords* consiste em descartar as palavras que pouco refletem no conteúdo de um documento ou são tão comuns que não distinguem nenhuma categoria dos documentos. Todas as palavras foram convertidas para minúsculas e acentos e caracteres especiais foram retirados.

Os atributos utilizados nessa pesquisa foram: grupos de uma a cinco palavras, telefones, URL's e valores monetários. Os demais atributos da pesquisa de Deng e Peng (2006) foram desconsiderados, como o tamanho da mensagem e o remetente. Esses atributos foram desconsiderados porque as mensagens utilizadas nessa pesquisa são mensagens enviadas por provedores de conteúdo. Essas mensagens possuem o tamanho maior quando se compara com mensagens enviadas de assinante para assinante, e os remetentes sempre são os mesmos. Cada um desses atributos selecionados contribui para o que se chama de probabilidade posterior no cálculo do teorema de Bayes. Em seguida, a probabilidade é calculada sobre todos os atributos de uma mensagem. O cálculo é realizado para ambos os casos, tanto para a mensagem ser spam, quanto para a mensagem não ser spam. A classificação é determinada a partir do maior valor das probabilidades de spam e não spam. Além disso, o filtro estará em constante atualização. A partir da chegada de novas mensagens, as probabilidades de cada uma das palavras são atualizadas, deixando, assim, cada vez mais precisa a detecção de mensagens spam e não spam.

4.2. Descrição do Algoritmo do Cliente implementado para o Sistema Operacional Android

O algoritmo do cliente foi desenvolvido para ser executado nos celulares que possuem o sistema operacional Android. Foram utilizados a linguagem Java SDK 1.5 do Android, e utilizando banco de dados SQLite. Nesta parte do projeto as pessoas poderão contribuir com as mensagens que recebem em seus celulares, indicando se são ou não spams. Quando a aplicativo é baixado e instalado, o mesmo lê todas as mensagens na caixa de entrada do celular do cliente e envia ao servidor os dados atualizados para serem incluídos na base de dados central do filtro. A partir desse momento, a cada nova mensagem que chegar ao celular, novas probabilidades são calculadas, e novos dados são enviados ao banco de dados do servidor.

4.3. Descrição do Algoritmo do Servidor

O algoritmo do servidor é a parte principal desse projeto. Ele contém toda a implementação do filtro de conteúdo. A cada nova mensagem que o algoritmo receber, são separados nos seguintes elementos: grupos de uma a cinco palavras e atributos. Após essa separação é realizado o cálculo da probabilidade dessa mensagem ser ou não spam. Para cada grupos de palavras e atributos obtidos em uma mensagem, é realizado

uma consulta na base de dados do filtro, identificando a incidência destes elementos como spam ou não spam. Posteriormente, é realizado o cálculo, utilizando a Fórmula (4) a seguir:

$$P(S \mid W) = \frac{P(W \mid S) \cdot P(S)}{P(W)} \qquad (4)$$

Após realizado o cálculo de cada um dos elementos da mensagem é realizado o cálculo da mensagem inteira ser spam, utilizando a Fórmula (5) abaixo.

$$P(S \mid W_i) = \prod_{t=1}^{n} P(s_t \mid W_i) \qquad (5)$$

O desenvolvimento do algoritmo ficou dividido em três módulos. No primeiro módulo, denominado Treinamento, foram inseridas uma lista de mensagens, spam e não spam. As probabilidades de cada um dos atributos e grupos de uma a cinco palavras são calculadas, classificando cada uma delas como spam ou não spam.

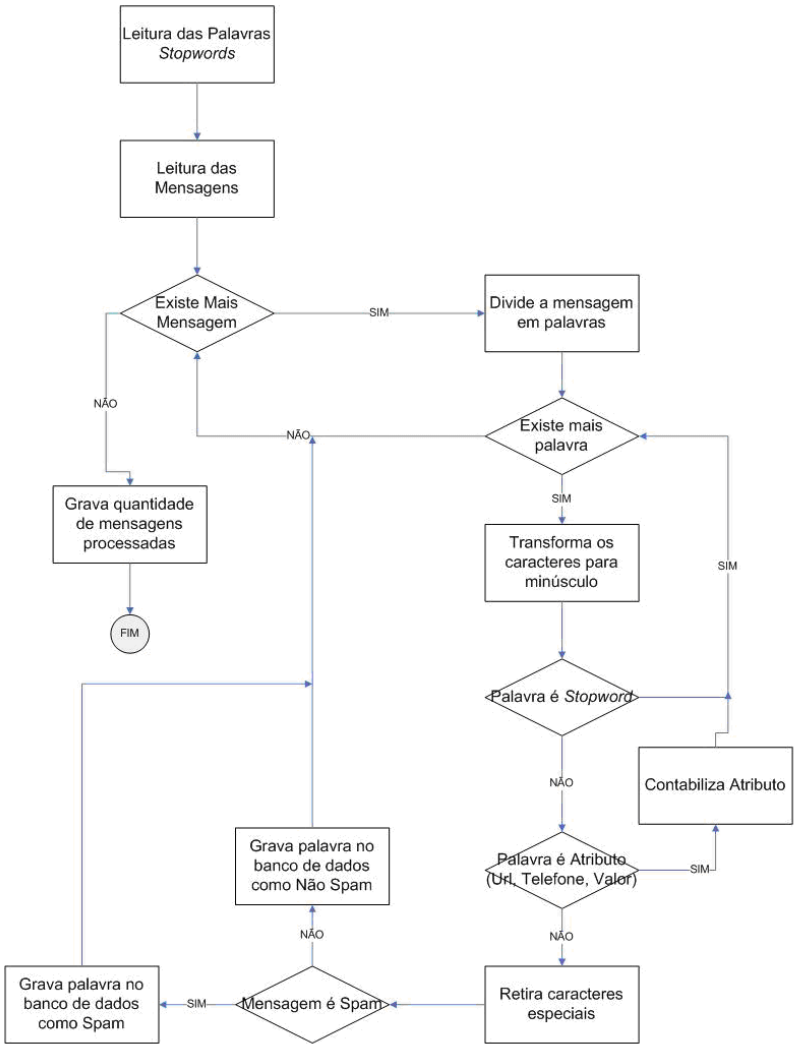


Figura 1. Fluxograma do Módulo Treinamento

No segundo módulo, denominado Classificação, o algoritmo recebe uma mensagem e a classifica como spam ou não spam. No terceiro módulo, denominado Aprendizado, os usuários que utilizarem o aplicativo no sistema operacional Android poderão contribuir com o filtro a partir das classificações realizadas por ele. O módulo Treinamento pode ser entendido melhor no fluxograma da Figura 1 e explicado melhor posteriormente.

O módulo Treinamento apresentado na Figura 1 apresenta o fluxograma de treinamento das mensagens utilizadas. Inicialmente foi realizado a carregamento dos *stopwords* na memória do servidor para utilização futura. Para cada mensagem lida foi realizado o processo de preparação da mensagem, onde todos os caracteres especiais, acentos e *stopwords* são retirados, e foi verificado se na mensagem existe algum atributo, como telefone, URL e valores monetários.

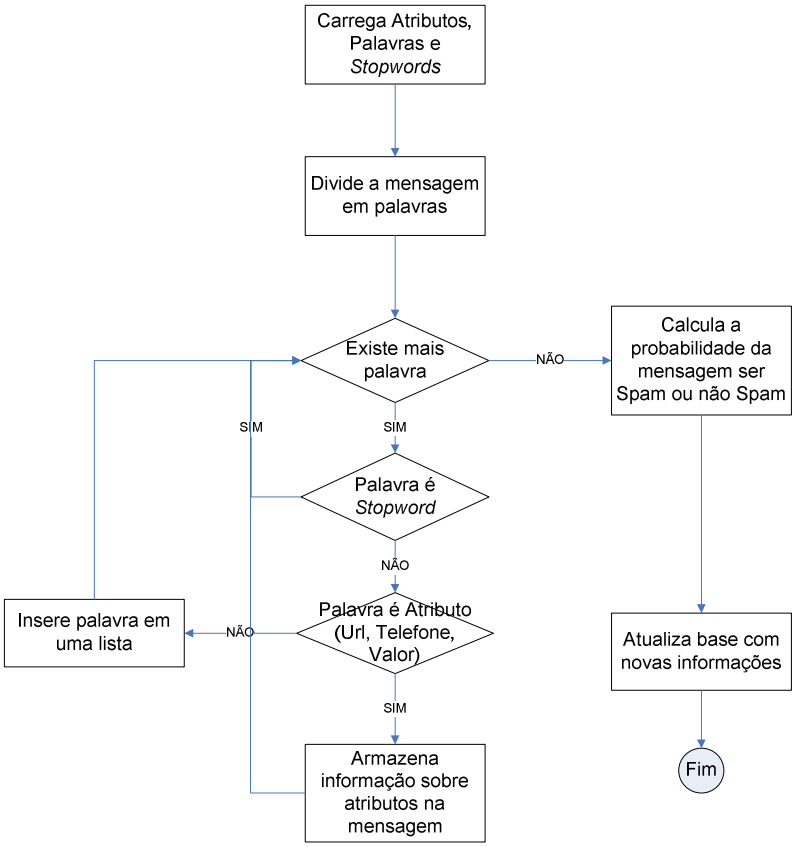


Figura 2. Fluxograma do Módulo Classificação e Aprendizado

O módulo Classificação e Aprendizado apresentado na Figura 2 apresenta o fluxograma de classificação da mensagem enviada. Inicialmente é realizado a carregamento dos *stopwords*, atributos e elementos na memória do servidor para utilização futura. A mensagem é preparada da mesma forma como demonstrado no processo da Figura 1, onde todos os caracteres especiais, acentos e stopwords são retirados, e é verificado se na mensagem existe algum atributo, como telefone, URL e valores monetários.

5. Experimentos e Resultados

Os experimentos foram realizados no filtro de conteúdo após a carga de 120.000 mensagens que foi realizado no processo de treinamento. Dessas 120.000 mensagens, 25.000 mensagens foram classificadas manualmente como spam e 95.000 mensagens foram classificadas manualmente como não spam. Essa carga realizada gerou 1.405.285 elementos, além dos atributos telefone, URL e valores monetários. Para realizar os experimentos foram obtidas mais 8.687 mensagens. Essas mensagens também foram classificadas manualmente, e dentre elas 8008 mensagens foram classificadas como não spam e 636 mensagens foram classificadas como spam. Essa classificação manual foi realizada para que após a obtenção dos resultados os mesmos possam ser conferidos e verificando assim o percentual de acerto do algoritmo. Os experimentos foram divididos em cinco partes. Na primeira parte dos testes, as 8.687 mensagens foram classificadas considerando apenas uma palavra e os atributos. Na segunda parte dos testes, as 8.687 mensagens foram classificadas considerando o grupo de uma a duas palavras, e os atributos. Na terceira parte dos testes, as 8.687 mensagens foram classificadas considerando o grupo de uma a três palavras, e os atributos. Na quarta parte dos testes, as 8.687 mensagens foram classificadas considerando o grupo de uma a quatro palavras, e os atributos. Na quinta parte dos testes, as 8.687 mensagens foram classificadas considerando o grupo de uma a cinco palavras, e os atributos.

Para realizar os experimentos do filtro de spam SMS, foi utilizado um equipamento com um processador Intel (R) Xeon (R), com dois processadores de 2.0 GHz, memória principal de 4 GB, memória secundária de 350 GB, sistema operacional Ubunbu 9.04 e banco de dados PostgreSQL 8.4. O tempo total gasto para este equipamento executar os testes chegou a 181,827 segundos na detecção de spams e não spams para 8.687 mensagens utilizando o agrupamento de uma a cinco palavras.

5.1. Resultados e Análises

A Tabela 1 apresenta os resultados para classificação de grupos de uma a cinco palavras e atributos. Os testes realizados para uma palavra e atributos apresentou o percentual de falsos positivos foi de 0,045% e o percentual de falsos negativos foi 0,044%. O desempenho total do algoritmo foi de 99,955% de acerto. Nessa parte do testes foram utilizados 69.515 grupos de uma palavra. O espaço utilizado para esses grupos foi de 0,49MB. Os testes realizados para o grupo de duas palavras e atributos apresentou o percentual de falsos positivos foi de 0,191% e o percentual de falsos negativos foi 0,007%. O desempenho total do algoritmo foi de 99,978% de acerto. Nessa parte do testes, foram utilizados 366.910 grupos de uma a duas palavras. O espaço utilizado para esses grupos foi de 4,38MB. Os testes realizados para o grupo de três palavras e atributos apresentou o percentual de falsos positivos foi de 0,209% e o percentual de falsos negativos foi 0,005%. O desempenho total do algoritmo foi de 99,9799% de acerto. Nessa parte do testes foram utilizados 717.550 grupos de uma a três palavras. O espaço utilizado para esses grupos foi de 11,05MB. Os testes realizados para o grupo de quatro palavras e atributos apresentou o percentual de falsos positivos foi de 0,218% e o percentual de falsos negativos foi 0,005%. O desempenho total do algoritmo foi de 99,9792% de acerto. Nessa parte do testes foram utilizados 1.073.356 grupos de uma a quatro palavras. O espaço utilizado para esses grupos foi de 19,95MB. Os testes realizados para o grupo de cinco palavras e atributos apresentou o percentual de falsos

positivos foi de 0,220% e o percentual de falsos negativos foi 0,005%. O desempenho total do algoritmo foi de 99,9790% de acerto. Nessa parte do testes foram utilizados 1.405.285 grupos de uma a quatro palavras. O espaço utilizado para esses grupos foi de 30,32MB.

Tabela 1. Resultados dos testes de grupos de uma, duas, três, quatro e cinco palavra e atributos

	Uma Palavra e Atributos	Duas Palavras e Atributos	Três Palavras e Atributos	Quatro Palavras e Atributos	Cinco Palavras e Atributos
Tempo em segundos do teste	53,815	99,041	131,117	148,856	181,827
Número de mensagens	8.687	8.687	8.687	8.687	8.687
Quantidade de mensagens spam	8.008	8.008	8.008	8.008	8.008
Quantidade de mensagens não spam	636	636	636	636	636
Falso positivo	29	122	133	139	140
Falso negativo	360	64	42	42	42
Grupos utilizados	69.515	366.910	717.550	1.073.356	1.405.285
Memória (MB)	0,49	4,38	11,05	19,95	30,32

Conforme demonstrado no gráfico da Figura 3, é possível perceber que o desempenho do filtro foi mais eficiente quando foi utilizado do grupo de até três palavras e atributos. A utilização do grupo de três palavras é mais eficiente por executar em um tempo menor que o grupo de quarto e cinco palavras, e por ter um índice de acerto melhor que o grupo de uma e duas palavras. Também vale destacar a diferença na utilização do grupo de uma palavra e o grupo de até duas palavras, onde o percentual de acerto aumentou significativamente. Quando foi utilizado o grupo de até quatro e cinco, o desempenho teve uma pequena queda.

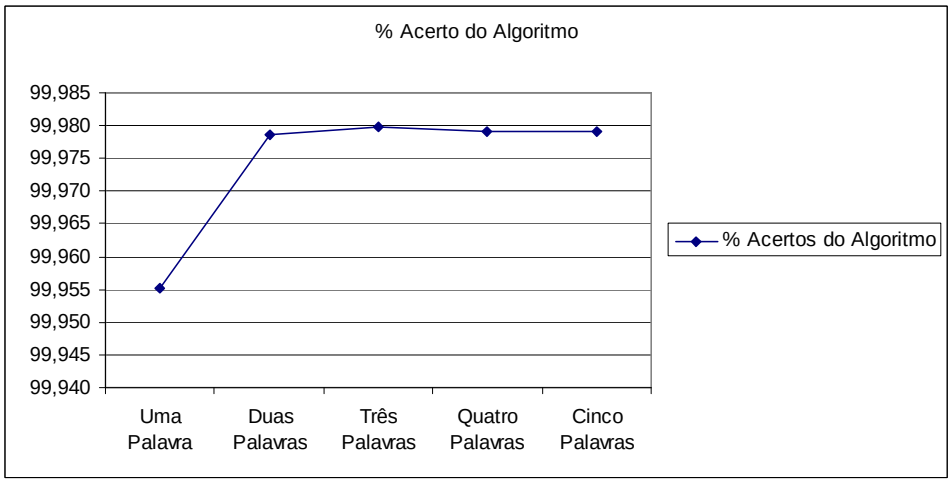


Figura 3. Percentual de acerto do algoritmo para o grupo de uma a cinco palavras

Além dos testes realizandos com 120.000 mensagens, foram realizados testes com 10.000 mensagens para uma comparação com a quantidade de mensagens utilizadas por Deng e Peng (2006). Dentre as 10.000 mensagens, 5.000 mensagens são

spam e 5.000 mensagens não spam. A Figura 4, apresenta os resultados obtidos com o treinamento com 10.000 mensagens e testes com 8.687 mensagens.

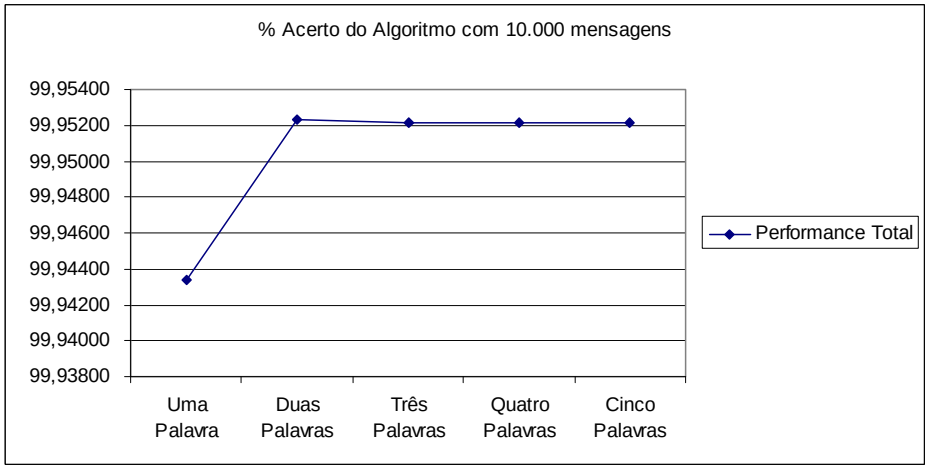


Figura 4. Percentual de acerto do algoritmo para o grupo de uma a cinco palavras com testes realizados com 10.000 mensagens

6. Conclusões e Trabalhos Futuros

A principal contribuição deste trabalho foi a implementação de um filtro de conteúdo para sistemas SMS baseado em classificador Bayesiano com agrupamento de palavras. Com este tipo de agrupamento de palavras, foi possível melhorar o percentual de acerto do algoritmo em comparação com a proposta de Deng e Peng (2006). Este trabalho foi motivado, principalmente, pela necessidade de se detectar e bloquear spams em ambientes reais de sistemas SMS de operadoras de telefonia celular. Como os testes foram realizados sobre mensagens reais, de uma operadora de telefonia celular, os resultados indicam que o filtro apresentado é altamente eficaz e consegue identificar e bloquear spams com quase 100% de acerto. Considera-se os resultados alcançados plenamente satisfatórios e o filtro totalmente possível de ser implementado em redes reais.

A diferença desta proposta para a de Deng e Peng (2006) está na implementação do algoritmo. Enquanto Deng e Peng (2006) usam apenas uma palavra, o filtro aqui proposto permite a combinação de uma a cinco palavras. Os testes para detecção de spams em um ambiente real foram feitos para 120.000 mensagens, enquanto Deng e Peng (2006) testaram apenas para 10.000 mensagens.

Os resultados mostraram que a utilização de grupos de palavras tornou o filtro mais eficiente na classificação de mensagens spam e não spam, principalmente para grupos de duas ou três palavras. A utilização de quatro e cinco palavras não obteve um resultado superior. O índice de acerto do filtro implementado chegou a 99,9799%, enquanto a proposta de Deng e Peng (2006) obteve 99,1% de acerto.

Quatro trabalhos futuros podem ser citados: (1) Extensão do filtro para todas as mensagens trafegadas na SMSC da operadora com o agrupamento de palavras, adicionando os atributos remetente e tamanho da mensagem, propostos por Deng e Peng (2006). (2) Implementação de um filtro de conteúdo com diversas classes. Dessa forma, o filtro ao invés de classificar as mensagens com apenas as classes spam e não spam

poderá classificar as mensagens por assunto, como por exemplo: promoção, esporte, financias, humor, políticas e religiosas. Dessa forma o usuário poderá liberar ou bloquear um determinado assunto. (3) Implementação de um filtro de conteúdo com classes por faixa etária. Dessa forma, o filtro, ao invés de classificar as mensagens com apenas as classes spam e não spam, poderá classificar as mensagens em faixas etárias dos usuários dos dispositivos móveis. Assim, os usuários dos dispositivos móveis que possuem idade abaixo dos 18 anos, por exemplo, não receberão mensagens com conteúdo ofensivo ou pornográfico. (4) Implementação de um filtro de conteúdo que faça uma tarifação diferenciada para o envio de mensagens promocionais ou propaganda. Nesse caso, a operadora, poderá tarifar dos provedores de conteúdo que enviam mensagens com propaganda de forma diferenciada.

Referências

ASSIS, J. M. C. Detecção de E-mails Spam Utilizando Redes Neurais Artificiais. Dissertação (Mestrado) — Universidade Federal de Itajubá - Programa de Pós-Graduação em Engenharia Elétrica, 2006.

BALINSKI, Ricardo. Filtragem de Informações no Ambiente do Direto. 2002. Dissertação (Mestrado em Informática) - Universidade Federal do Rio Grande do Sul, Porto Alegre.

BOAS, Roberta de Matos Vilas. Faturamento com SMS deve crescer globalmente, mas no Brasil preço alto dificulta uso. Disponível em < http://web.infomoney.com.br/templates/news/view.asp?codigo=1241084&path=/suas financas/estilo/tecnologia/>. Acesso em: 19 out. 2008.

CORMACK, G.; LYNAM, T. Spam corpus creation for TREC. In: Proceedings of the Second Conference on Email and Anti-Spam. Mountain View, CA, USA: CEAS, 2005. Disponível em: <http://www.ceas.cc/papers-2005/162.pdf>. Acesso em: 05 nov. 2009.

CRANOR, L. F. LAMACCHIA, B. A. Spam! In: Commun. ACM. New York, NY, USA: ACM, 1998. v. 41, p. 74–83. ISSN 0001-0782.

DENG, Wei-Wei., PENG, Hong. Research on a Naive Bayesian Based Short Message Filtering System. Machine Learning and Cybernetics, 2006 International Conference on, p. 1233-1237, Aug. 2006.

GARNER, Philip, MULLINS, Ian, EDWARDS, Reuben e COULTON, Paul. Mobile Terminated SMS Billing – Exploits and Security Analysis. Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on, p. 1319-1324, jun. 2008.

HE, P. SUN, Y. ZHENG, W. WEN, X, Filtering Short Message Spam of Group Sending Using CAPTCHA, Knowledge Discovery and Data Mining, 2008. WKDD 2008. International Workshop on, p. 558 – 561, Jan. 2008.

HE, Peizhou, WEN, Xiangming e ZHENG Wei. A Novel Method for Filtering Group Sending Short Message Spam. Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on, p. 60–65, Aug. 2008.

KANTARDZIC, M, Data Minimg, Concepts, Models, Methods and Algorithms. J. B. Speed Scientific School University of Louisvile, IEEE Computer Society, Sponser 2003

MING L, YUNCHUN L. WEI L. Spam Filtering by Stages. Convergence Information Technology, 2007. International Conference on. p. 2209 - 2213, Nov. 2007

SAHAMI, M. DUMAIS, S. HECKERMAN, D. HORVITZ E. A Bayesian Approach to Filtering Junk E-mail, AAAI Workshop on Learning for Text Categorization, July 1998, Madison, Wisconsin. AAAI Technical Report WS-98-05

SHAHREZA, M. Verifyin Spam SMS y Arabic CAPTCHA, Information and Communication Technologies, 2006. ICTTA '06. 2nd, p. 78 – 83, 2006.

SHAHREZA, S. M.H., An Anti-SMS-Spam Using CAPTCHA. Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on, p. 318–321, Aug. 2008.

SILVA, Alission Marques Da. Utilização de Redeis Neurais Artificiais para Classificação de Spam. Dissertação (mestrado) – Centro Federal de Educação Tecnológica de Minas Gerais. 126f. Mar. 2009.

ZHANG, H. WEN, X; HE, P. ZHENG, W. Dealing with Telephone Fraud Using CAPTCHA, Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on, p. 1096 – 1099, June 2009.

XV Workshop de Gerência e Operação de Redes e Serviços

♦

Sessão Técnica 4

Gerenciamento de Redes Móveis, Sem Fio e de Sensores

Proposta De Uma Métrica de Roteamento Para Redes *Wireless Mesh* com Tráfego *Voip*

Cleverton Juliano Alves Vicentini[1], **Roberson Cesar Alves de Araujo**[1], **Mauro Sergio Pereira Fonseca**[1]

[1]Programa de Pós-Graduação em Informática Aplicada - (PPGia),
Pontíficia Universidade Católica do Paraná (PUCPR)
Caixa Postal 17.315 – 80.215-901 – Curitiba – PR – Brasil

{cleverton,roberson.araujo,mauro.fonseca}@ppgia.pucpr.br

Abstract. *Search for the best routes in a wireless network is not a trivial task, several studies are carried out in order to find better protocols and routing metrics that adapt to Wireless Mesh network. It is seen that most studies are aimed to find solutions for running mesh networks in any topology, however not always a metric or protocol will work correctly in different environments. This work demonstrates a new routing metric called FK (Factor-K) that aims to operate in wireless mesh networks in low mobility scenarios with VoIP traffic. Its performance was evaluated and compared with the ML (Minimum Loss) metric. These simulations indicate that metric FK provides better performance in the network model used with VoIP traffic.*

Resumo. *Buscar melhores rotas em uma rede sem fio não é uma tarefa trivial, diversos trabalhos realizam estudos afim de encontrar melhores protocolos e métricas de roteamento que se adequem a redes Wireless Mesh. É visto que grande parte dos estudos objetivam a busca de soluções para redes sem fio do tipo Mesh de forma que funcionem em qualquer topologia, porém nem sempre um protocolo ou métrica irá operar de forma satisfatória em diversos ambientes. O presente trabalho demonstra uma nova métrica de roteamento entitulada FK (Factor-K) que objetiva atuar em redes Mesh em cenários de baixa mobilidade com tráfego Voip. Seu desempenho foi avaliado e comparado com a métrica ML (Mininum Loss). As simulações realizadas mostram que a métrica FK propicia um melhor desempenho no modelo de rede utilizado com tráfego Voip.*

1. Introdução

Devido ao constante avanço das redes do tipo *Wireless*, que fornecem acesso sem fio a computadores e dispositivos móveis através de ondas de rádio, e por sua facilidade de implantação sem a necessidade de uma estrutura de rede cabeada, esta tecnologia tende a ser cada vez mais explorada por universidades e grandes empresas. Como o objetivo de redes sem fio é prestar melhores serviços, recentemente surgiu uma tecnologia chave: as redes em malha sem fio (*Wireless Mesh Networks)* que tem como principal atrativo seu custo reduzido para cobertura de áreas relativamente grandes onde é financeiramente inviável a instalação de uma infra-estrura de rede cabeada. Universidades tem utilizado a plataforma *Wireless Mesh* de forma a prover serviços de Internet a seus alunos e funcionários além de interligar prédios com a comunicação sem fio [ReMesh 2005] [Tsarmpopoulos et al. 2005].

Redes *Wireless Mesh* são compostas de roteadores sem fio e clientes *Mesh*, onde roteadores *Mesh* tem mínima ou nenhuma mobilidade formando o *backbone* da rede. Uma característica relevante dos roteadores *Mesh* fixos é o fato de não necessitarem realizar a gestão de energia, desta forma geralmente possuem poder de processamento maior que roteadores móveis. Características desejáveis nas redes *Mesh* são auto-organização e auto-configuração, tais características possibilitam a manutenção das conexões dos roteadores presentes na rede de forma automática, visando a inclusão de novos roteadores na rede para o aumento da área de cobertura da rede *Mesh* [Akyildiz et al. 2005]. De uma forma geral, os protocolos de roteamento utilizados em redes *Wireless Mesh* são adaptações de protocolos de roteamento para redes *ad hoc*. Porém, o fato dos protocolos de roteamento *ad hoc* serem desenvolvidos para redes onde nós são móveis, podem causar instabilidades se utilizados nas redes *Wireless Mesh*.

Métricas de roteamento é um assunto relevante nas redes *Mesh*. As métricas objetivam melhorar o desempenho da rede atuando geralmente na diminuição da taxa de perda e aumento da vazão da rede. Cada métrica de roteamento é estruturada para diferentes cenários, e é verificado que métricas de roteamento em redes sem fio de baixa mobilidade não é um tópico muito abordado no âmbito de redes *Mesh*. Este artigo propõe uma métrica de roteamento que utiliza as informações referentes a perda de pacotes de dados de um nodo, parametrizando o peso de cada enlace da rota. Seu objetivo é obter menores taxas de perda, menor atraso e maior vazão nas redes *Mesh* estacionárias com tráfego *Voip*. Seguindo este critério, rotas alternativas serão definidas com o objetivo de oferecer melhor desempenho a rede. A métrica apresentada neste documento é intitulada *Factor-K* (FK).

A motivação que leva ao estudo de uma métrica de roteamento que se adapte a redes *Wireless Mesh* com tráfego de Voz, deve-se ao crescimento e popularização da tecnologia *Voice over Internet Protocol* (VoIP). Este crescimento justifica-se pelas reduções significativas com os custos em telefonia. O cenário escolhido para os testes foi o Campus da Pontifícia Universidade Católica do Paraná (PUC-PR), por ser um cenário viável de implatação destas tecnologias.

Este documento está organizado da seguinte forma: Seção 2 apresenta os trabalhos relacionados. A seção 3 descreve a métrica *Factor-K*. A seção 4 apresenta o cenário de simulação e parâmetros utilizados na simulação, seção 5 apresenta os resultados obtidos e por fim seção 6 contém a conclusão desta pesquisa.

2. Trabalhos Relacionados

Esta seção aborda alguns trabalhos relacionados que utilizam a arquitetura das redes *Wireless Mesh*. Descreve o comportamento dos protocolos de roteamento *wireless* e aborda algumas métricas de roteamento utilizadas em redes *Mesh*.

2.1. Projetos que Utilizam a Arquitetura Wireless Mesh

O projeto *RoofNet* [Bicket et al. 2005] é desenvolvido pelo *Massachusetts Institute of Technology* (MIT) na cidade de Cambridge. O *RoofNet* encontra-se em uma área urbana bem povoada, localizada próxima ao MIT, onde inicialmente foram instalados 37 nodos *Mesh*, este número é incrementado a medida que mais voluntários participam do projeto.

Para o roteamento do projeto *RoofNet* foi utilizado um procolo baseado no DSR (*Dynamic Source Routing*), nomeado de Srcr. Os protocolos diferem pelo fato do DSR utilizar a métrica do número de *hops* e o protocolo Srcr utiliza a métrica ETT (*Estimated Transmission Time*), uma variação da métrica ETX (*Estimated Transmission Count*). Sendo assim, o protocolo procura por rotas com menor valor de ETT. Os estudos do grupo MIT demonstraram que a arquitetura *Wireless Mesh Network* é viável de implantação.

O projeto *ReMesh* [ReMesh 2005] atua objetivando implantar uma rede *Mesh* de acesso comunitário em um dos *campi* da Universidade Federal Fluminense, para assim fornecer acesso banda larga para: funcionários, alunos e professores que residem nas proximidades do campus. O projeto está sendo desenvolvido pelo Departamento de Telecomunicações (DET) e o Instituto de Computação (IC) da Universidade Federal Fluminense (UFF), sendo financiado pela RNP (Rede Nacional de Ensino e Pesquisa). Foi definido para o projeto como protocolo de roteamento o OLSR (*Optimized Link State Routing Protocol*), por apresentar-se mais estável neste tipo de rede e roteadores sem fio *linksys WRT54G* equipados com software livre (*OpenWRT*) [OpenWrt 2009].

O protocolo OLSR utilizado no *ReMesh* não está em sua forma original. A equipe do *ReMesh* implementou uma modificação no cálculo das métricas, gerando um novo protocolo o ML *(Minimum Loss)*. A proposta OLSR-ML define-se como a probabilidade de transmissão com sucesso entre dois nós. Os estudos da UFF demonstraram que o procolo ML obteve melhores resultados quando comparado a métrica ETX (descrita na sessão 3).

Outro projeto relevante que utiliza a arquitetura *Mesh* é o *VMesh*. Este projeto iniciou com uma rede *Mesh* na cidade de Volos, na Grécia, atendendo interesses relacionados a pesquisa, ensino e atividades particulares do Departamento de Engenharia de Computação da Universidade de Tessaly [Tsarmpopoulos et al. 2005]. A arquitetura do projeto *VMesh* é composta por vários dispositivos estacionários e móveis. Os dispositivos estacionários são os roteadores sem fio, localizados no alto de prédios e telhados para obter uma melhor conectividade, permitindo que dispositivos clientes obtenham conexão local para possibilitar acesso ao resto da rede. O protocolo de roteamento utilizado no *VMesh* é o OLSR. O *VMesh* possibilitou um avanço nas pesquisas em redes *Mesh*, demonstrando a viabilidade de implantação deste tipo de rede. O desempenho da rede foi satisfatório levando em conta as limitações da tecnologia. O custo do conjunto *hardware* e *software* é de certa forma baixo. A transferência de dados no projeto VMesh é realizada pelo melhor esforço [Tsarmpopoulos et al. 2005].

2.2. Protocolos de Roteamento para Redes *Wireless*

Protocolos de roteamento para redes *Wireless* são classificados em reativos, pró-ativos e híbridos. Os protocolos de roteamento reativos realizam a descoberta da rota sob demanda, ou seja, somente quando necessitam enviar informações a rota é solicitada. Este processo é utilizado geralmente em redes de alta mobilidade, pois evita o desperdício de energia dos nodos. Os protocolos de roteamento pró-ativos realizam o processo de descoberta dos nós de forma constante, deste modo, quando ocorre a necessidade da transferência de dados a rota já é conhecida para utilização imediata. Estes tipos de protocolos podem ser adequados para redes *Mesh* de baixa mobilidade, onde não existe a limitação de energia pois os roteadores são geralmente fixos e com alimentação contínua. Os protoco-

los de roteamento híbridos fazem a concatenação dos conceitos pró-ativos e híbridos, dividindo o cenário em zonas de roteamento de forma que em determinadas zonas o princípio pró-ativo é utilizado e em outros momentos o princípio reativo é aplicado.

Mesmo não utilizando todos os recursos que as redes *Wireless Mesh* podem oferecer, como o poder de processamento e a não limitação de energia [Passos and Albuquerque 2007], alguns protocolos de roteamento desenvolvidos para redes *ad-hoc* foram implantados em redes *Wireless Mesh*. São exemplos de protocolos *ad-hoc* utilizados em redes *Wireless Mesh* os protocolos: DSR (*Dynamic Source Routing*)[Johnson et al. 2003] e AODV *(Ad Hoc On-Demand Distance Vector)* [Perkins et al. 2003].

Nas redes *wireless* o grande número de mensagens de controle disseminadas pelos nós podem vir a prejudicar a estabilidade da rede, alguns protocolos de roteamento pró-ativos objetivam diminuir esta sobrecarga de mensagens na rede. Um exemplo é o protocolo de roteamento OLSR (*Optimized Link State Routing Protocol*) [Clausen and Jacquet 2003], que utiliza a abordagem de *Multipoint Relays* (MPR). Os MPR são um conjunto de vizinhos selecionados por um determinado nó que terão a tarefa de retransmitir mensagens de controle pela rede. A utilização da abordagem MPR evita a inundação de *broadcasts*, auxiliando na estabilidade da rede.

2.3. Métricas de Roteamento

Redes *Ad Hoc* normalmente utilizam a quantidade de saltos como métrica de roteamento. Tal métrica é adequada a redes *Ad Hoc* pelo fato que novas rotas de uma rede devem ser encontradas de forma rápida [Campista et al. 2008]. As redes *Wireless Mesh*, por possuírem uma topologia onde os nós formadores do *backbone* são geralmente fixos, uma rota com menor número de saltos pode não ser a melhor escolha. Desta forma, foram desenvolvidos algumas métricas de roteamento diferentes da métrica de quantidade de saltos, que podem ser integradas aos protocolos de roteamento utilizados nas *Wireless Mesh Networks*.

A primeira métrica proposta para as *Wireless Mesh Networks* (WMN) é a *Expected Transmission Count* (ETX) [Campista et al. 2008]. A métrica ETX mede de forma continua a taxa de perda de ambos os sentidos entre cada nó e seus respectivos vizinhos, monitorando as taxas de perda dos enlaces através de troca de mensagens periódicas, assim como em enlaces alternativos para garantir o uso da melhor rota. Esta métrica calcula o peso da rota através da soma dos ETX's de cada enlace, que será utilizado pelo protocolo de roteamento para o cálculo da melhor rota.

A métrica *Expected Transmission Time* (ETT) [Bicket et al. 2005], foi desenvolvida como uma extensão da métrica ETX. A ETT considera a taxa de transmissão utilizada para realizar com precisão a qualidade dos enlaces. Seu objetivo é estimar o valor do atraso do canal, realizando a concatenação do ETX do enlace com a taxa de transmissão do nó. Duas métricas alternativas a métrica ETX são: ML (*Minimum Loss*) [Passos and Albuquerque 2007] e AP (*Alternative Path*) [Mascarenhas et al. 2008]. A métrica ML objetiva a busca de caminhos com menores probabilidades de perda de pacotes mesmo que necessite utilizar um número maior de saltos que a métrica ETX. Já a métrica AP considera a quantidade de vizinhos de cada rota visando escolher a rota que contenha o menor número de nós vizinhos pois, segundo Mascarenhas

[Mascarenhas et al. 2008], quanto maior a quantidade de vizinhos maior a interferência da rota.

Ambas as métricas ML e AP demonstraram um melhor desempenho e menores taxas de perda de pacotes quando comparadas a métrica ETX. É interessante destacar que a maioria das métricas de roteamento utilizam a métrica ETX ou pequenas variações da mesma para cálculo das tabelas de roteamento [Passos and Albuquerque 2007]. Seguindo este mesmo paradigma, a métrica FK descrita na seção 3 será uma variação da métrica ETX.

Os estudos descritos nesta seção demonstraram que as redes *Wireless Mesh* são viáveis de implantação, e estão em processo de crescimento, sendo assim possibilitando a pesquisa de novas tecnologias na área. Os projetos *RoofNet* e *ReMesh* fizeram a utilização do OLSR com adição de métricas de roteamento em seus projetos. Ambos os projetos verificaram que o OLSR em sua forma original pode não ser a melhor escolha para redes *Mesh*, pelo fato de que em sua forma original o OLSR escolher rotas com menores saltos. Já o projeto *VMesh* optou pelo OLSR em sua forma original, desta forma podendo comprometer o desempenho da rede.

3. Extensão Proposta para a Métrica ETX

A métrica ETX utiliza para o cálculo da qualidade do enlace o inverso do resultado gerado pelo produto do *Link* Direto (*forward delivery ratio(df)*) pelo *Link* Reverso (*reverse delivery ratio (dr)*), onde o *Link* Direto é responsável pelo envio dos pacotes *hello* e o *Link* Reverso é responsável pelos reconhecimentos positivos (ACKs) [Albuquerque et al. 2006]. Assim o ETX de um enlace $a \rightarrow b$ é definido como o inverso da probabilidade de transmissão com sucesso de um pacote através deste enlace como ilustra a equação 1.

$$ETX_{ab} = \frac{1}{P_{ab}} \tag{1}$$

Para o cálculo de uma rota com múltiplos saltos com utilização da métrica ETX, o valor de ETX total da rota é obtido através da soma do valor de ETX de cada salto. Por exemplo: em uma rota $a \rightarrow c$, será feita a soma do ETX do enlace $a \rightarrow b$ com ETX do enlace $b \rightarrow c$, como citado em [Passos and Albuquerque 2007], o ETX de uma rota $a \rightarrow n$ é definida por:

$$ETX_n = \sum_{i=0}^{n-1} \frac{1}{P_{a_i a_{i+1}}} \tag{2}$$

Onde $P_{a_i a_{i+1}}$ ilustra a probabilidade de transmissão com sucesso de um pacote entre os nós $a_i a_{i+1}$.

Para criação da métrica *Factor-K* (FK) foi realizada a alteração do cálculo original da métrica ETX. Os estudos demonstram que a métrica ETX considera apenas os pacotes de *hello* para o cálculo da métrica. O diferencial da métrica proposta neste artigo é além de considerar os pacotes *hello*, a métrica FK considera também os pacotes de dados reais dos nós *Mesh*. Desta maneira a nova métrica atribui ao *Link* Direto (df) da métrica ETX, o valor dos pacotes de dados perdidos do nó correspondente, para desta forma setar os

pesos para cada enlace da rota, detectando assim enlaces com altas taxas de perdas de pacotes. A expressão 3 LP (*Lost Packets*) é responsável por extrair os valores dos pacotes de dados perdidos pelos nós *Mesh*.

$$LP = ((totalpkts - lostpkts)/totalpkts) \tag{3}$$

Onde *totalpkts* corresponde ao total de pacotes enviados e *lostpkts* corresponde aos pacotes perdidos pelo nodo correspondente. Ao atribuir o LP ao *Link* Direto de ETX obtém-se a nova métrica Factor-K como ilustra a expressão 4.

$$FK_{ab} = \frac{1}{P_{((a+lp)b)}} \tag{4}$$

Para o cálculo de uma rota com múltiplos saltos a métrica *Factor-K* realiza o somatório dos valores de FK de cada enlace afim de obter o custo total de cada rota. A equação 5 denota este cálculo.

$$FK_n = \sum_{i=0}^{n-1} \frac{1}{P_{((a_i+lp)a_{i+1})}} \tag{5}$$

A métrica FK terá seu melhor desempenho em redes com alto tráfego de dados como pode ser visto na seção 4, pois quando o enlace apresentar altas taxas de perda de pacotes a métrica irá retornar um peso maior para o atual enlace, forçando o protocolo de roteamento a escolha de uma rota alternativa.

4. Cenário de Simulação

O cenário utilizado para as simulações foi o campus da PUC-PR (Figura 1), que é composto por vários blocos e áreas de estacionamento entre os blocos. Com o objetivo de avaliar o comportamento da métrica FK, as simulações foram executadas no *Network Simulator 2* [NS2 2010], utilizando-se extensões para o OLSR e a métrica ML desenvolvidas para o NS-2 [Cordeiro et al. 2007].

Foram realizadas 10 simulações com diferentes sementes, o tráfego foi gerado através de transmissões *Voip* (UDP) e FTP (TCP). As simulações são compostas por 12 fluxos *Voip*, que representam 6 chamadas *Voip*, juntamente com tráfego de *background* FTP. O número de 6 chamadas *Voip* justifica-se por ser um limiar entre 4 e 9 chamadas [Aguiar et al. 2007].

O protocolo de roteamento utilizado nas simulações foi o OLSR, amplamente utilizado em redes *Mesh*. Para comparar os resultados da métrica *Factor-K* apresentada neste documento, foi utilizada a métrica *Minimum Loss* [Passos and Albuquerque 2007] no mesmo cenário de simulação. Esta escolha se dá pelo fato da métrica ML ser amplamente utilizada nas WMN [ReMesh 2005] e com resultados superiores a métrica ETX.

A Figura 1 ilustra o campus da PUC-PR com os roteadores *Mesh* sendo representados pelos círculos amarelos, as linhas contínuas indicam as chamadas *Voip* e as linhas tracejadas indicam o tráfego de *background*. Os blocos foram numerados de 1 a 10,

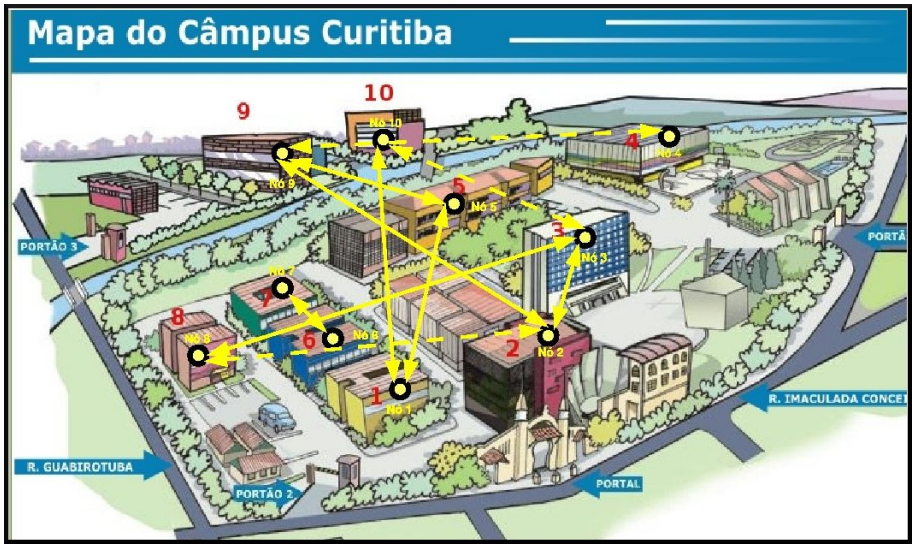


Figura 1. Campus PUC-PR Adaptado de [PUC-PR 2010]

ficando: 1-CTHC, 2-Biblioteca Central, 3-Administração Central, 4-Quadras Poliesportivas, 5-Bloco Acadêmico, 6-CCET, 7-CCBS, 8-CCJS, 9-Parque Tecnológico e 10-PPGIA. A tabela 1 descreve as localizações dos nós pelo cenário de simulação conforme figura 1.

Tabela 1. Parâmetros de Simulação

Posição dos nodos em metros					
Indentificação do Nó	**Eixo X**	**Eixo Y**	**Indentificação do Nó**	**Eixo X**	**Eixo Y**
1. CTHC	160,00	485,00	6. CCET	628,00	320,00
2. Biblioteca Central	305,00	277,00	7. CCBS	570,00	440,00
3. Administração Central	340,00	226,00	8. CCJS	780,00	480,00
4. Quadras Poliesportivas	270,00	32,00	9. Parque Tecnológico	918,00	597,00
5. Bloco Acadêmico	476,00	200,00	10. PPGIA	968,00	550,00

As chamadas *Voip* são compostas por dois fluxos, pois a aplicação tem fluxo bidirecional e os fluxos de ida e volta não trafegam pelos mesmos pontos. O trafego de *background* (FTP) foi gerado através do Modelo de Pareto [NS2 2010], para caracterizar tráfego em rajadas, com valores *default*. O *codec* utilizado para as simulações foi o G.729, pois seu consumo de banda é de 8 Kbps, desta forma é o mais utilizado nas redes sem fio [Cordeiro et al. 2007]. A tabela 2 demonstra os parâmetros da simulação.

Tabela 2. Parâmetros de Simulação

Parâmetros	Valores
Protocolo de Roteamento	OLSR
Métricas	Factor-K e Minimum Loss
Tempo de Simulação	50 Segundos
Padrão Utilizado	IEEE 802.11b
Modelo de Propagação	Shadowing
Modelo das Antenas	Omnidirecional, 18dB de ganho
Path Loss Exponent	2,7
Shadowing deviation	4.0dB
Área de Simulação	1000m x 1000m
N° Nós Mesh	10

O intervalo de confiança para análise dos resultados foi de 95% calculado conforme [Jain 1991]. Os valores escolhidos para avaliação dos resultados foram: *jitter*, atraso, vazão e probabilidade de bloqueio.

5. Resultados Obtidos

A figura 2 ilustra os resultados de atraso para os 12 fluxos *Voip* (2 fluxos por chamada) obtidos nas simulações. A métrica *Factor-K* demonstra melhor desempenho a partir do momento em que ocorre o aumento de tráfego na rede, diminuindo consideravelmente o atraso. Pode-se observar que na primeira chamada Voip a métrica FK demonstra uma alta taxa de atraso, isso justifica-se pelo fato da chamada ser iniciada entre pontos muito distantes na rede.

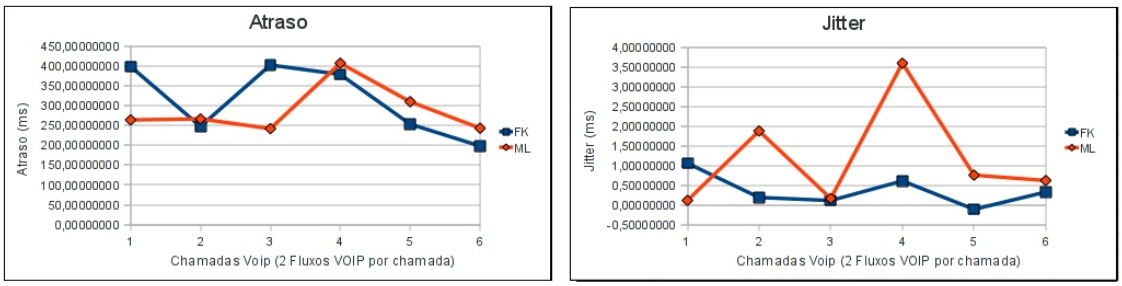


Figura 2. Atraso e Jitter

Os resultados para *jitter* também ilustrados na figura 2, demonstram o melhor comportamento da métrica FK, consequência dos menores atrasos obtidos com esta métrica. Tanto o atraso quanto o *jitter* diferem para fluxos da mesma chamada, isto ocorre pelo fato dos fluxos tomarem rotas diferentes, devido à interferências dos outros nós.

A figura 3 apresenta os resultados de vazão. Observou-se que a métrica FK obteve melhor comportamento perante a métrica ML. A distância entre os nós influencia na vazão dos dados, pois quanto menor a distância maior é a vazão. Com relação a probabilidade de bloqueio a métrica FK novamente teve menores resultados em relação a ML, não excedendo os 0,28. A métrica ML teve probabilidade máxima de 0,49.

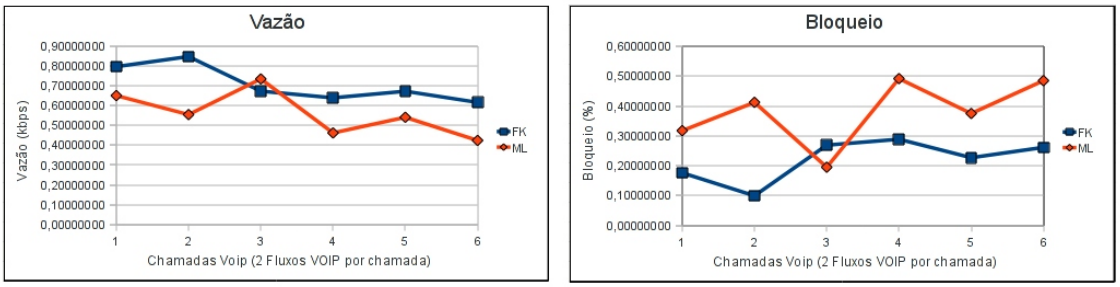


Figura 3. Vazão e Bloqueio

Através da análise dos gráficos apresentados nas figuras 2 e 3, conclui-se que o comportamento da métrica FK obteve melhores resultados que a métrica ML. Estes resultados mostram que o fato da métrica FK considerar os pacotes de *hello* juntamente

com os pacotes de dados perdidos pelos nodos nos enlaces da rede, melhora o desempenho de redes *Mesh* com alto tráfego de dados *Voip*.

6. Conclusão do Artigo

Com o crescimento das redes sem fio do tipo *Mesh*, a necessidade de novas tecnologias para estes tipo de rede torna-se necessário. O tema redes *Mesh* está sendo amplamente estudado devido à complexidade do tema. Desta maneira as redes sem fio do tipo *Mesh* podem desenvolver um maior potencial com relação a serviços oferecidos e desempenho.

Neste artigo, o objetivo foi discutir as métricas de roteamento que constituem uma das diversas áreas de pesquisa sobre este tipo de rede. A importância das métricas de roteamento são fundamentais em redes *Mesh* e *Ad-Hoc*, pois, os enlaces e rotas necessitam estar em processo constante de avaliação, porém, interferindo o mínimo possível no desempenho da rede. Quando a rede *Mesh* dispõem de tráfego *Voip* juntamente com tráfego TCP, o tema métricas de roteamento torna-se ainda mais desafiador.

Este trabalho apresentou uma nova métrica de roteamento denominada FK, que aprimora o cálculo de rotas nas redes *Mesh* com tráfego *Voip*. A métrica FK utiliza como base o cálculo de probabilidades de transmissões feito pela métrica ETX juntamente com os pacotes de dados reais para cálculo das rotas, desta forma quando o enlace estiver com altos índices de tráfego de pacotes a métrica FK irá retornar ao protocolo de roteamento um peso maior para esta rota, forçando a busca de rotas alternativas.

As simulações demonstraram que a métrica FK obteve melhores resultados perante a métrica ML com relação a *jitter*, perda de pacotes, atraso e vazão no cenário utilizado. Este desempenho se deve ao fato da métrica FK utilizar além do cálculo de probabilidades de transmissões, os pacotes de dados perdidos pelo nodo, de forma a detectar o instante em que um enlace se encontra com altas taxas de perda de pacotes, forçando a busca de rotas com menor tráfego.

Na sequência das pesquisas poderão ser utilizados outros pacotes de dados como taxa de erro e fila para o cálculo da métrica FK. Outra possibilidade seria testar o comportamento da métrica FK em redes com maiores números de nós e tráfegos mais intensos.

Referências

Aguiar, E., Bittencourt, P., Moreira, W., and Abelém, A. (2007). Estudo comparativo de protocolos de roteamento para redes mesh na regiao amazônica. *XXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC - Sessão de Artigos Curtos II*.

Akyildiz, I., Wang, X., and Wang, W. (2005). Wireless Mesh Networks: a survey. In *Computer Networks and ISDN Systems*, pages 445–487.

Albuquerque, C. V. N., Saade, D. C. M., Passos, D. G., Teixeira, D. V., Leite, J., Neves, L. E., and Magalhães, L. C. S. (2006). Gt-Mesh - Rede Mesh de Acesso Universitário Faixa Larga Sem Fio - Relatório Técnico 3. (RT-3 1-118).

Bicket, J., Aguayo, D., Biswas, S., and Morris, R. (2005). Architecture and evaluation of an unplanned 802.11 b mesh network. In *Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 31–42. ACM New York, NY, USA.

Campista, M., Esposito, P., Moraes, I., Costa, L., Duarte, O., Passos, D., de Albuquerque, C., Saade, D., and Rubinstein, M. (2008). Routing metrics and protocols for wireless mesh networks. *IEEE network*, 22(1):6.

Clausen, T. and Jacquet, P. (2003). RFC3626: Optimized Link State Routing Protocol (OLSR). *RFC Editor United States*.

Cordeiro, W., Aguiar, E., Abélem, A., and Stanton, M. (2007). Providing Quality of Service for Mesh Networks Using Link Delay Measurements. *Proceedings of 16th International Conference on Computer Communications and Networks, p.991-996*.

Jain, R. (1991). *The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling*. Wiley New York.

Johnson, D., Maltz, D., Hu, Y., and Jetcheva, J. (2003). The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). *IETF Mobile Ad Hoc Networks Working Group, Internet Draft, work in progress*, 15.

Mascarenhas, D., Rubinstein, M., and Sztajnberg, A. (2008). Uma nova métrica para protocolos de roteamento em redes em malha sem fio. *XXVI Simpósio Brasileiro de Redes de Computadores - SBrT*.

NS2 (2010). Network Simulator-NS2, Home Page, http://www.isi.edu/nsnam/ns.

OpenWrt (2009). OpenWrt - Wireless Freedom . Disponível em: http://openwrt.org.

Passos, D. and Albuquerque, C. (2007). Proposta, Implementaçao e Analise de uma Metrica de Roteamento Multiplicativa para Redes em Malha Sem Fio. *Anais do XXVII Congresso da SBC*, pages 1935–1944.

Perkins, C., Belding-Royer, E., and Das, S. (2003). IETF RFC 3561, Ad hoc ondemand distance vector (AODV) routing [S].

PUC-PR (2010). Mapa Campus PUC-PR, Home Page, http://www.vestibular.pucpr.br/pseletivo/unificado2008/mapa.html.

ReMesh (2005). Universidade Federal de Fluminense. 2005. Disponível em: http://mesh.ic.uff.br.

Tsarmpopoulos, N., Kalavros, I., and Lalis, S. (2005). A low-cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers. In *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005. First International Conference on*, pages 92–97.

Abaré: Um Framework para Implantação, Monitoramento e Gerenciamento Coordenado e Autônomo para Redes em Malha sem Fio

Billy Anderson Pinheiro[1-3], Vagner de Brito Nascimento[1-3], Eduardo Cerqueira[1-4], Antônio Jorge Gomes Abelém[1-3], Augusto Neto[5]

Grupo de Estudos em Redes de Computadores e Comunicação Multimídia (GERCOM)[1]
Programa de Pós-Graduação em Ciências da Computação (PPGCC)[2]
Universidade Federal do Pará (UFPA)[3]
Faculdade de Engenharia da Computação – UFPA[4]
Universidade Federal de Goiás (UFG)[5]

{billy,vagner,cerqueira,abelem}@ufpa.br, augusto@inf.ufg.br

Abstract. *The Wireless Mesh Networks (WMNs)have been gaining ground as a solution to provide last mile indoors and outdoors Internet access, because of their technical and economic feasibility. However, the existence of open source and proprietary approaches that are not interoperable and the delay in the standardization process make deployment of a large-scale WMN time-consuming and complex. This paper presents an extension of the framework Abaré with autonomic capability and performance evaluation results regarding load balance issues. Abaré defines a set of components and practices in order to optimize the implementation and management of WMN systems, as well as to provide autonomic features in routers to decrease and facilitate the manager workload.*

Resumo. *As redes em malha sem fio vêm se consagrando como solução para o acesso de última milha em ambientes internos e externos, devido sua viabilidade técnica e econômica. No entanto, a existência de soluções de código aberto e proprietárias que não são interoperáveis e a demora no processo de padronização torna a implantação de uma rede em malha sem fio de larga escala uma tarefa demorada e complexa. Este artigo apresenta uma extensão do framework Abaré com capacidade autonômica e resultados de desempenho no que diz respeito ao balanceamento de carga. Abaré define um conjunto de componentes e práticas para otimizar a implantação e gerenciamento de redes em malhas sem fio, bem como prover características autonômicas nos roteadores com o objetivo de reduzir e facilitar o trabalho do administrador .*

1. Introdução

As Redes em Malha Sem Fio (*Wireless Mesh Networks* - WMNs) surgem como uma solução atraente para prover ubiquidade e conectividade à última milha. A cooperação entre os nós permite o uso eficiente da largura de banda e a redução de custos operacionais [Campista *et al* 2008]. No entanto, este tipo da rede ainda sofre com a falta de padronização, o que acarreta em desperdício de recursos e tempo [IEEE draft p802.11s d4.0 2009].

Como forma de aproveitar o crescente mercado das WMNs várias empresas, como a Motorola e Cisco já desenvolveram soluções denominadas *pré-mesh* para facilitar a comunicação nas redes, mas o custo elevado e a falta de interoperabilidade destes equipamentos impedem sua utilização em ambientes de grande escala [Motorola 2009] [Cisco 2009].

Como alternativa às soluções proprietárias, equipamentos com suporte a IEEE 802.11 podem ser usados com o *firmware* modificado, usando uma distribuição Linux [OpenWRT 2009] [DD-WRT 2009]. Este tipo de solução permite a fácil criação de ambientes digitais, possibilitando a distribuição e gerenciamento de novos serviços para equipamentos sem fio e a captação de novos clientes. Vários projetos mostram que o uso desta solução é viável, como o *Vmesh* na Grécia [Vmesh 2009] e o *Remesh* no Brasil [Remesh 2009].

Outra característica esperada pelas WMNs e que será fundamental para a expansão das mesmas é a autonomia. Segundo Khalid [Khalid *et al* 2009] a computação autonômica é um conceito inspirado nos sistemas biológicos, que pretende diminuir a complexidade de administrar grandes sistemas heterogêneos através da capacidade de auto-gerenciamento, minimizando a intervenção humana. Dentre as propriedades que habilitam as capacidades autonômicas de um sistema, podemos destacar a auto-configuração, auto-otimização, auto-recuperação e auto-proteção [Kephart e Chess 2003].

A fim de suprir os requisitos esperados pelas WMNs no que diz respeito à gerência eficiente, auto-organização e interoperabilidade, este artigo estende o *framework* Abaré[1]. Esta solução descreve métodos para auxiliar a implantação e o gerenciamento de WMNs com base em informações coletadas dos roteadores e das condições da rede, provendo facilidades para a gestão por parte do administrador e possibilitando a existência de nós autônomos que possamos tomar decisões sem a necessidade da interferência humana. Avaliação de um protótipo do Abaré foi realizada em ambiente real, sendo executados testes de carga com o intuito de comprovar a viabilidade e comportamento.

Este trabalho está estruturado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados a gerenciamento e WMN. Na seção 3 é apresentado o *framework* Abaré. A Seção 4 apresenta a aplicação do *framework*. Na Seção 5 são apresentados os testes realizados e os resultados obtidos. Finalmente, a Seção 6 apresenta as conclusões gerais e sugere possíveis trabalhos futuros.

2. Trabalhos Relacionados

O *Distributed Architecture for Monitoring Multi-hop Mobile NetworksDistributed Ad-hoc Monitoring Network* (Damon) é um sistema para monitoramento distribuído de redes de sensores *ad-hoc* que foi proposto por [Ramachandran *et al* 2004]. Nele existem agentes usados para coletar informações da rede e enviar os dados para os repositórios. Vale ressaltar que esse algoritmo é dependente do protocolo de roteamento *Ad-hoc On-Demand Distance Vector* (AODV) para sua operação, ou seja, é impossível o uso deste *framework* em uma rede que use OLSR [Aguiar et al. 2007] ou outro protocolo de roteamento, reduzindo desta forma a

[1] Em tupi-guarani: Amigo do Homem.

flexibilidade do sistema.

Jardosh [Jardosh *et al* 2008] projetou o SCUBA, um *framework* para visualização interativa de problemas em WMNs de grande escala. Neste *framework*, várias métricas são reunidas em um banco de dados através de um nó *gateway*. Esta informação é usada para gerar uma visão interativa. Uma implementação inicial do *framework* foi testado em uma rede com 15 nós que mostrou a viabilidade do *framework* para fornecer o serviço de visualização. É importante ressaltar que apenas a visualização é fornecida por este *framework,* não fornecendo nenhum mecanismo de gerência.

Riggio [Riggio *et al* 2007] propôs um *framework* distribuído para WMNs chamado JANUS. Os testes realizados foram em uma WMN do tipo cliente [Aggelou *et al* 2009] usando microcomputadores com MCL (*Mesh Connectivity Layer*) instalada[Microsoft 2009]. Apesar dos testes positivos, a proposta atual é restrita à tarefa de monitorar a rede, sendo necessário o uso de outra ferramenta de gerenciamento para configura a rede.

Mesh-Mon é um *framework* proposto e implementado por Nanda e Kotz [Nanda e Kotz 2008] que realiza o monitoramento da rede para auxiliar o administrador com suas tarefas. Este sistema de gerenciamento é definido como sendo escalável e distribuído, capaz de detectar automaticamente e recuperar falhas na rede. No entanto, o *framework* é reduzido às tarefas de monitoramento da rede e executa algumas ações automaticamente se o comportamento da rede é diferente de um padrão que foi definido estaticamente pelo autor.

MobiMESH é uma implementação para WMNs que fornece um abrangente *framework* de análise do comportamento em tempo real , incluindo suporte avançado de roteamento considerando múltiplos rádios, alocação de canais, bem como de gerenciamento [Capone *et al* 2007]. No entanto, este *framework*, como acontece na maioria das outras propostas, não oferece suporte a módulos adicionais que poderiam torná-los adaptáveis à realidade da rede ao longo do tempo.

Após a análise dos trabalhos relacionados, podemos observar que a implantação, monitoramento e gerenciamento de WMNs, tanto de forma autônoma como assistida, são tarefas importantes para o sucesso das mesmas e para atender a esses requisitos, o *framework* Abaré foi proposto e é apresentado na próxima seção.

3. Framework Abaré

O *framework* Abaré [Pinheiro *et al* 2009] tem como objetivo desenvolver um sistema de especificação e padronização para a gerência autonômica de WMNs. Desta forma, o Abaré visa facilitar os processos de implantação e manutenção de WMNs em grande escala. Ele foi concebido utilizando o conceito de OpenMesh, que são WMNs criadas com a utilização de equipamentos IEEE 802.11 convencionais alterando seu *firmware* para uma distribuição Linux embarcada. Além disto, é utilizado um algoritmo de roteamento dinâmico [Moreira *et al* 2007] com o esquema de endereçamento proposto por Tsarmpopoulos [Tsarmpopoulos *et al* 2005] em uma rede em malha seguindo a arquitetura infra-estruturada. Os elementos que compõem esta solução são descritos de maneira detalhada, bem como os passos necessários para a implantação em [Pinheiro et al. 2009].

A primeira versão deste *framework* veio para suprir às necessidades básicas para a implantação e gerência da rede. Porém, foi observado a necessidade de uma maior autonomia por parte do Agente Roteador, que na primeira versão deste framework estava localizado dentro dos roteadores, de maneira a permitir que os roteadores possam tomar decisões sem a necessidade de contato com o Abaré Core.

Para viabilizar este comportamento autônomo, o Agente Roteador foi substituído por um *middleware* chamado Middrouter que irá desempenhar as funções antes oferecidas pelo Agente Roteador, bem como viabilizar a autonomia dos roteadores na tomada de decisão. Para possibilitar a inserção do Middrouter foi necessário estender a arquitetura do Abaré como é apresentado na Figura 1.

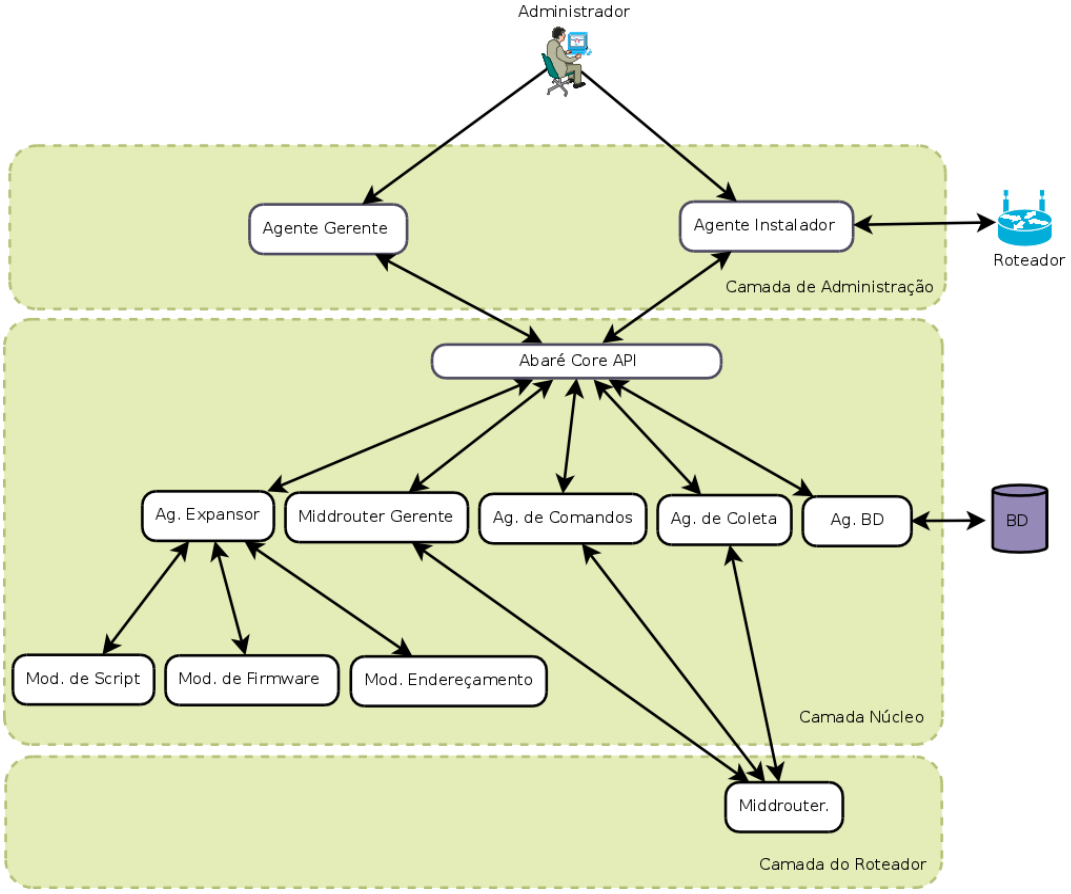


Figura 1: Abaré Framework

O *framework* foi desenvolvido de forma modular e possui três (3) camadas: administração, que é responsável pela interação com o administrador; Núcleo, que representa o centro do sistema onde a parte lógica e o armazenamento das informações estão localizados e a Camada do Roteador, que permite o acesso ao roteador para comunicação direta com o sistema operacional de cada nó da rede e adiciona a característica autonômica ao *framework*. A descrição de cada componente é apresentada a seguir:

- Agente Instalador - É o responsável por fazer as mudanças de *firmware* nos roteadores, executar a configuração inicial destes e armazenar os dados sobre cada roteador no Abaré Core API.

- Agente Gerente - Responsável por fornecer uma interface onde, após a devida autenticação, o administrador pode interagir com o sistema e usar os recursos oferecidos pelo Abaré Core. Em outras palavras, esta é a interface para gestão do sistema e sua implementação deve ser independente do sistema operacional e linguagem de programação.
- Abaré Core API - É o núcleo do sistema, responsável pela obtenção e gestão das informações de todos os componentes do *framework*. Ele deve fornecer funcionalidades, geralmente em formato de *Webservice*, que poderão ser utilizadas pelos Agentes Instalador e Gerente.
- Agente BD - Responsável pela leitura e escrita das informações no banco de dados.
- Agente de Coleta - Requisita informação sobre tráfego, hardware e tabelas de roteamento ao Middrouter e as envia para o Abaré Core API.
- Agente de Comandos - Responsável pelo envio de comandos para o Middrouter. Normalmente, ele é utilizado para tarefas administrativas que precisem de intervenção humana;
- Middrouter Gerente - Este é o responsável por controlar o Middrouter e modificar seus parâmetros. Através dele é possível inserir novos coletores e agentes de decisão, bem como agendar ações a serem tomadas pelos roteadores de forma autônoma.
- Agente Expansor - Permite a extensão do *framework* através da adição de novos módulos, fornecendo abstração suficiente para permitir o desenvolvimento rápido de novos recursos. Estes são módulos que já são definidos por padrão no *framework*:
    - Módulo de Endereçamento: Coordena os IDs dos roteadores e realiza a separação das redes e IPs utilizados;
    - Módulo de Scripts: Gera os scripts com os comandos que são repassados para o Agente de Comandos, que por sua vez, envia os comandos para serem executados nos roteadores.
    - Módulo de Firmware: Obtém os *firmwares* inseridos pelo administrador e fornece-os de acordo com as necessidades do Agente de Instalação.
- Middrouter - É responsável por responder às solicitações do Agente de Coleta, fornecendo as informações solicitadas no formato XML (*eXtensible Markup Language*). É preciso também aceitar os comandos enviados pelo Agente de Comando e executá-los nos roteadores, além de prover a parte autônoma do sistema. Este agente é dividido em seis (6) camadas, como na Figura 2, e suas funcionalidades são descritas a seguir:
    - Entrada e saída: Responsável pela recepção dos pedidos e por encaminhá-los para a camada correta dependendo do tipo de dados recebidos. É também responsável por enviar os resultados dos comandos executados e das métricas coletadas;
    - Parse XML: Recebe informações em XML da camada superior e identifica

qual o tipo da requisição, caso seja de coleta esta é encaminhada para o coletor selecionado, caso seja um comando ele é enviado ao Comandos. Na direção oposta, ele recebe as informações coletadas e as converte em XML para que a camada superior possa enviá-las;

- Comandos: Recebe e executa os comandos enviando uma resposta positiva ou negativa relativa à sua execução;
- Coletores: É um conjunto de pequenos módulos responsáveis pela coleta de informações e o envio para a camada superior. Quando um pedido chega ao Parse XML, apenas o nome do coletor é fornecido para que este seja acionado. Uma vez que o módulo coletor é acionado, ele deve executar esse pedido e responder com a informação solicitada. Assim, é fácil a integração dos novos módulos de coleta, sendo necessário apenas inserir o novo módulo no roteador e que a entidade que precisa usar a métrica fornecida pelo módulo saiba seu nome;

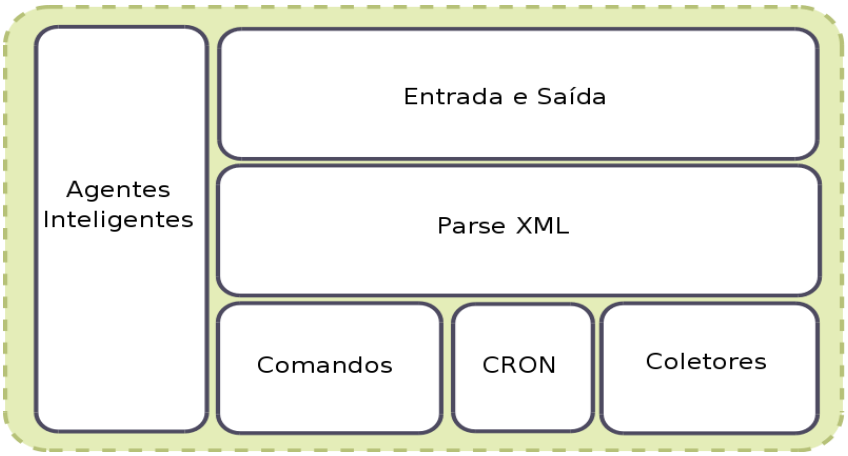


Figura 2: Middrouter

- CRON: Este é o elemento responsável por agendar ações no Middrouter, chamando os elementos de tomada de decisão de acordo com regras temporais estabelecidas.
- Agentes Inteligentes: Estes são os responsáveis por prover a autonomia dos roteadores, permitindo que estes possam tomar decisões com base em informações coletadas e executando comandos de acordo com a análise dos dados recebidos.

4. Aplicação do Framework

O uso do *framework* Abaré visa tornar os passos de implantação e manutenção de uma rede WMN uma tarefa sistemática e auxiliada por *software*, ou seja, criar uma modelagem que possa ser facilmente executada com a ajuda de uma aplicação que atenda aos requisitos do *framework*. A aplicação do Abaré em um ambiente real foi realizadaseguindo os princípios OpenMesh como apresentada na Figura 3.

A Figura 3 exibe os Middrouters nos roteadores e os computadores usados para a implantação e gestão da rede. É possível identificar no *backbone* da WMN a presença

do Middrouter que são incorporados em cada roteador *mesh*. O Abaré Core está localizado fora do *backbone* e conectado a WMN através dos *gateways mesh*.

O Abaré Core está configurado no mesmo equipamento que hospeda o banco de dados e o servidor de autenticação, mas isso não é obrigatório. A única exigência é que eles devem estar na mesma sub-rede, de preferência, conectados por meio cabeado, para evitar problemas de segurança e disponibilidade. A equipe de suporte da Figura 3 representa os usuários dos Agentes Instalador e Gerente que podem ser instalados em terminais fixos ou móveis já que o Abaré Core é concebido como um *Web Service* que fornece independência de plataforma e de linguagem de programação [Park e Lee 2003].

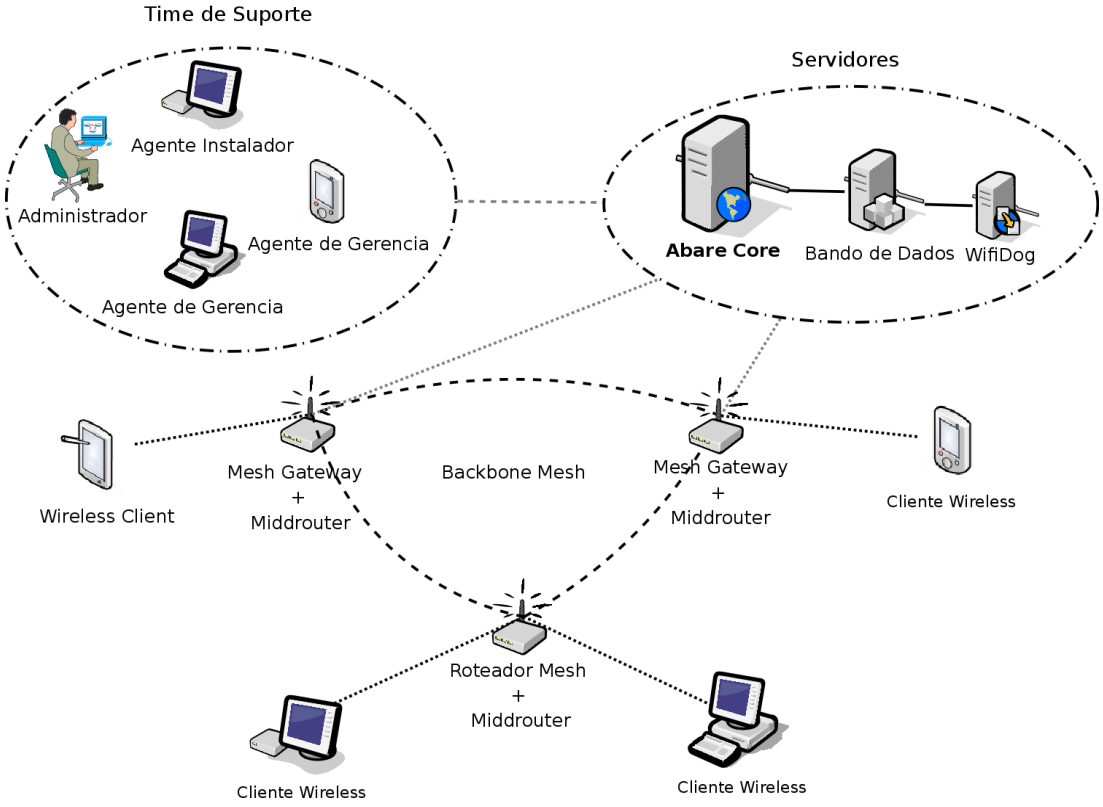


Figura 3: Aplicação do Abaré

Para avaliar o *framework*, foram desenvolvidos protótipos contendo todas as funcionalidades do Agente Instalador, os módulos de *firmware*, Controle e Scripts, um protótipo do Agente Gerente com as interfaces para acessar os módulos do core e o Middrouter. Quase todos os protótipos empregados nas avaliações foram desenvolvidos em linguagem Python[2], com a tecnologia XMLRPC[3] e OpenSSL[4] para a troca segura de mensagens, suporte para autenticação e a utilização de GTK[5] (GIMP toolkit) para a interface gráfica do usuário. A única exceção foi no Middrouter, pois as limitações de hardware impostas pelo equipamento impossibilitavam a utilização de um Web Service

[2] http://www.python.org
[3] http://www.xmlrpc.com
[4] http://www.openssl.org/
[5] http://www.gtk.org/

normal, com isso, foi necessário o desenvolvimento de um Web Service embarcado, feito sob medida para os dispositivos utilizados nos testes, sendo preciso implementar as bibliotecas necessárias para prover um Web Service.

Desta forma, o Middrouter foi desenvolvido utilizando a linguagem C. Devido à impossibilidade de utilização de bibliotecas XMLRPC ou SOAP convencionais, desenvolvemos um pequeno servidor HTTP para atender as requisições dos clientes sob o protocolo HTTP 1.0 [Berners-Lee *et al* 1996]. Além disto, foi implementada a biblioteca XML para realizar o tratamento das requisições XMLRPC. Estas implementações juntas, deram origem ao Middrouter com 32KB de tamanho, compilado para a arquitetura MIPS (*Microprocessor without Interlocked Pipeline Stages*), atendendo aos padrões de comunicação XMLRPC.

Para validar a utilização da nova arquitetura do Abaré, foram realizados testes tendo como foco o Middrouter. O cenário de testes foi a rede em malha da Universidade Federal do Pará (UFPA), que foi implantada em uma área que possui prédios com altura média de oito metros, com predominância de árvores de grande porte e copas largas, típicas da região amazônica. Possui também altos índices pluviométricos. A Figura 4 apresenta o *backbone* instalado da rede em malha da UFPA.

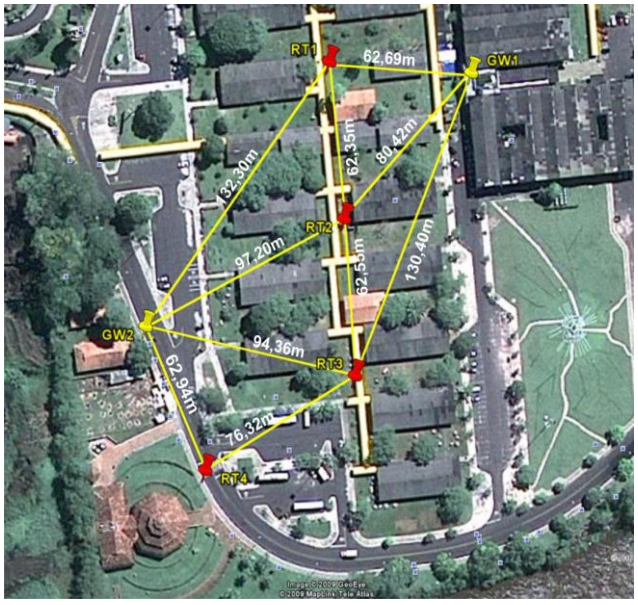


Figura 4: Backbone da rede em malha da UFPA

A rede em malha localizada na UFPA possui seis kits para redes em malha sem fio. Esses kits são compostos de caixa hermética para comportar os roteadores sem fio e uma antena omnidirecional de 18.5dBi de ganho. Os roteadores sem fio utilizados na rede são da marca Linksys e modelo WRT54GL. Estes possuem as configurações necessárias, para a utilização do *firmware* OpenWRT, sendo o mesmo baseado no sistema operacional Linux para sistemas embarcados. Segue abaixo, as configurações dos dispositivos.

- Arquitetura MIPS;
- Chipset Broadcom 5352EKPB;
- CPU speed: 200MHz;

- Memória Flash: 4MB;
- Memória RAM: 16MB;
- Interface Wireless: Broadcom BCM43xx – 802.11b/g;

5. Experimentos e Resultados

5.1 Teste de Carga

Para validar a parte de coletas do Middrouter e verificar seu comportamento em um sistema real foi realizado um teste de carga. Nele foram realizadas sucessivas requisições para um dos coletores presentes no Middrouter. O coletor em questão é o *get_mem_used*, que retorna a quantidade de memória utilizada. A intenção do teste era verificar a variação do tempo de resposta de acordo com o aumento do numero de requisições. Foram realizadas 10 execuções com um intervalo de confiança de 95% para cada número de requisições, no caso: 1, 2, 3, 4, 5, 10, 20 e 40.

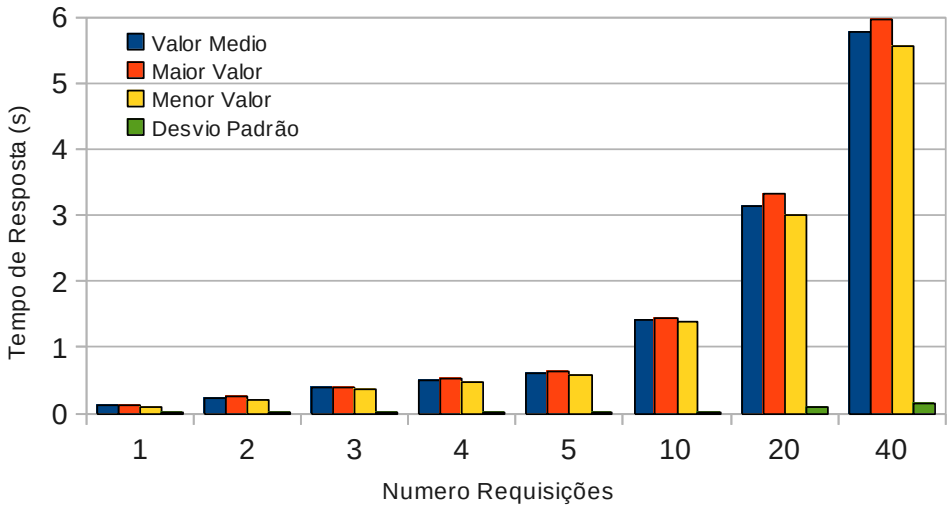


Figura 5: Tempo de Resposta do Middrouter

Na Figura 5 é possível perceber que o Middrouter pode responder as 40 requisições simultâneas em um tempo inferior a 6 segundos. É possível observar também um crescimento proporcional do tempo de resposta, uma vez que todos os pedidos são atendidos dentro dos limites de processamento do sistema.

5.2 Teste com o Agente Inteligente.

Uma das características mais importantes do Middrouter é a existência de agentes inteligentes que possibilitam a tomada de decisão por parte do roteador, ou seja, tornam possível a autonomia do roteador para coletar, analisar e tomar uma ação de forma autônoma.

Para validar este agente, foi implementado um simples agente de balanceamento de carga para demonstrar o funcionamento da parte autônoma do Middrouter. Os seguintes elementos foram desenvolvidos, utilizando os princípios propostos pelo Abaré:

- **ifstat** – É um coletor que foi implementado para monitorar a vazão;

- **ch_gw** – É um agente que troca o *gateway* do roteador hospedeiro caso ele receba uma ordem vinda de um dos *gateways*.
- **lb_gw** – É um Agente Inteligente, ele faz o uso do ifstat para monitorar a vazão, caso o número ultrapasse um limiar estabelecido ele envia uma ordem para alguns roteadores trocarem sua tabela de rota, alterando seu *gateway*, evitando uma sobrecarga em um determinado *gateway*.

No roteadores RT1, RT2 e RT3 foram implantados o **ch_gw** e no *gateway* GW1 o **ifstat** e o **lb_gw**. O CRON do Middrouter foi utilizado para agendar a execução do agente **lb_gw** em intervalos de tempo de 3 segundos. Para estes testes os roteadores RT4 e o GW2 não foram usados, sendo este último apenas usado como *gateway* alternativo em um dos testes. Todos os testes apresentados a seguir foram realizados 10 vezes, para gerar uma melhor confiabilidade nos testes.

Primeiramente foi realizado um teste com cada roteador isoladamente, para verificar a vazão máxima de cada um. Foi utilizada a ferramenta *Iperf* para gerar 8MB (Mega Byte) de dados que foram enviados usando o Protocolo de Controle de Transporte (*Transport Control Protocol* - TCP). O servidor ficou localizado na rede externa, ligado aos *gateway*s via Ethernet 100Mbits, o cliente estava dentro de cada roteador. A Figura 5 mostra os resultados obtidos.

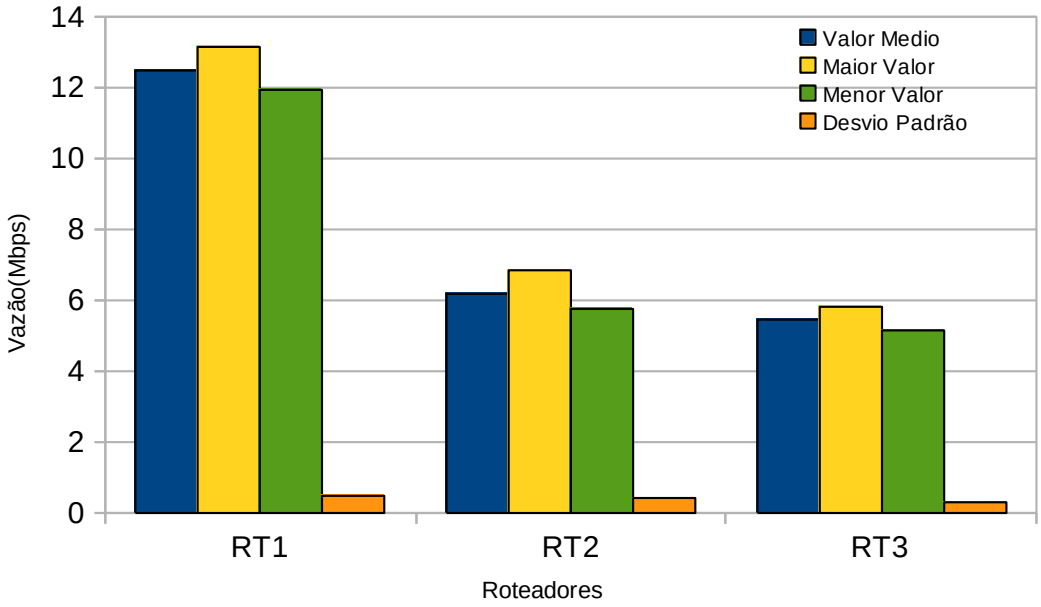


Figura 6: Vazão Individual dos Roteadores

É possível verificar os valores de 12.44Mbps, 6.18Mbps e 5.42Mbps para os roteadores RT1,RT2 e RT3 respectivamente. Atribuímos estas diferenças a fatores como distância e obstáculos que precisam ser vencidos pelo sinal de cada roteador. A partir dos dados coletados vimos que 12Mbps por segundo é o limite que estes roteadores conseguem alcançar através do GW2.

Com essas informações parametrizamos o **lb_gw** para alterar as rotas dos outros roteadores caso o valor da vazão do GW2 alcançasse 7Mbps, para ter uma margem que possa sustentar a comunicação com os demais roteadores que continuaram dependentes desse *gateway*.

Foram os três roteadores que de maneira concorrente fizeram requisições de um arquivo de 8MB para o servidor *iperf*, que está na rede externa como descrito anteriormente. Diante do trafego gerado o **lb_gw** foi ativado desencadeando a troca do *gateway* de um dos roteadores. A Figura 6 mostra os resultados obtidos:

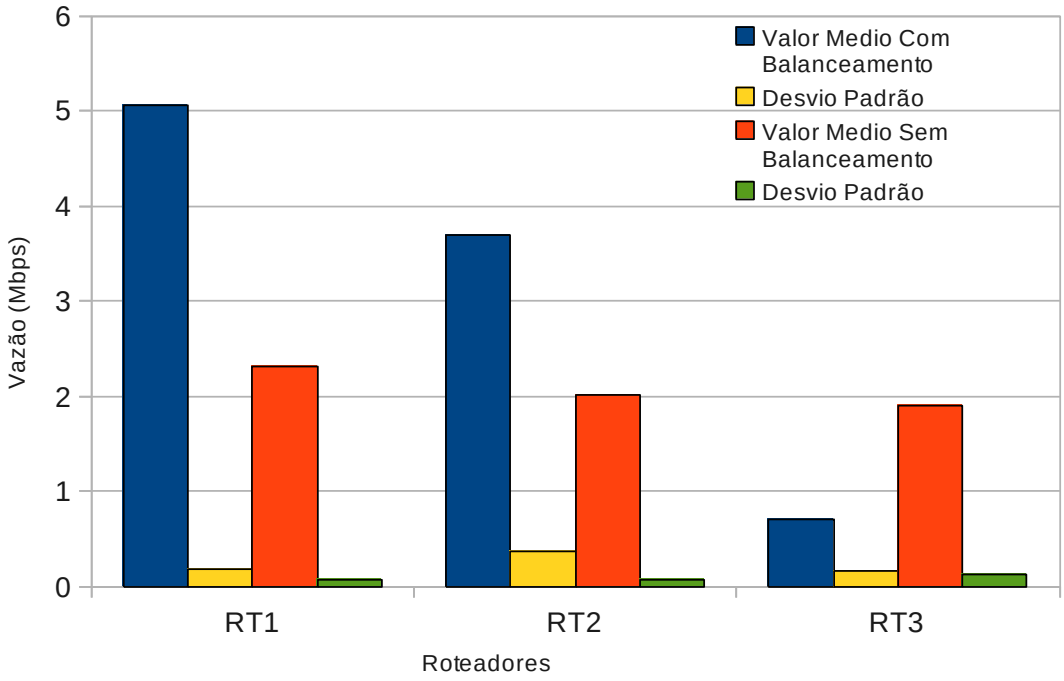


Figura 7: Vazão com os fluxos começando simultaneamente

É possível identificar, com o uso do **lb_gw**, uma melhora de 45.63% e 54.35% nos tráfegos do RT1 e RT2, respectivamente, porém o RT3 sofreu uma degradação em sua vazão. Isto ocorreu, pois o Agente **lb_gw** alterou a tabela de rotas do RT3 redirecionando-o para outro *gateway*, no entanto a sessão TCP foi perdida visto que a rede não implementa um tratamento para esta troca de *gateways* [Ito *et al* 2009].

Diante destas informações foi realizado um terceiro teste com os mesmo parâmetros do segundo, porém iniciando o tráfego do RT3, três segundos após os demais, desta forma a mudança de roteamento não quebraria a sessão TCP, pois ela ocorreria antes da sessão ser iniciada.

Na Figura 8 é possível perceber uma melhoria de 56.56% no trafego do RT3, uma vez que o TCP não sofre a quebra de sessão, promovendo o balanceamento de carga, ainda de maneira simples, pois esta não é a proposta do artigo. Com estes teste foi possível mostrar as facilidades proporcionadas pelo *framework*, que viabilizam a criação de outros módulos e agentes que resolvam problemas específicos, como balanceamento de carga, gerência de mobilidade entre outros.

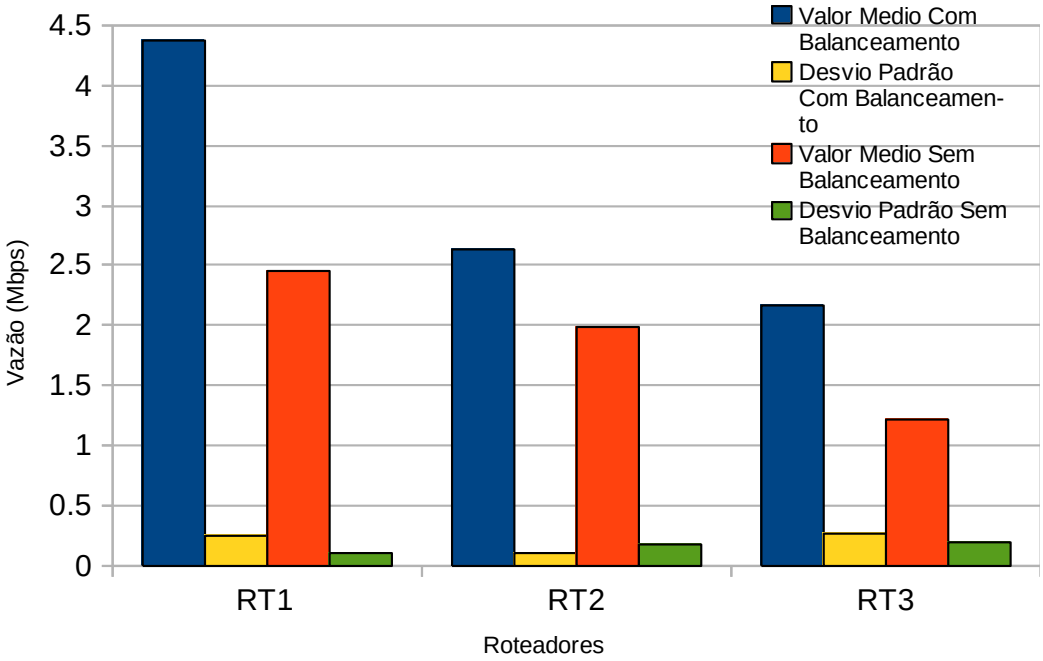


Figura 8: Vazão com os fluxos começando em tempos diferentes

É importante ressaltar que toda a comunicação entre os roteadores já é oferecida pelas camadas de entrada e saída e pelo parse XML, que abstraem a complexidade envolvida, deixando o desenvolvedor focado apenas na solução do problema principal.

6. Conclusões e Trabalhos Futuros

A implantação e gerenciamento são tarefas importantes para WMNs. Apesar de sua importância, apenas o monitoramento e poucas tarefas de configuração têm sido realizadas pelos *framewoks* existentes. Neste artigo, apresentamos uma nova arquitetura para o Abaré, levando em conta os aspectos de implantação e gerencia, bem como propiciando características autonômicas aos roteadores.

Este *framework* visa incentivar o desenvolvimento de ferramentas de gerência, uma vez que fornece a base teórica necessária para a sua criação, por especificar e padronizar os elementos de gerencia de uma WMN, dado que um dos maiores obstáculos para implantação em larga escala de Redes OpenMesh é a falta de ferramentas que possam auxiliar neste processo. A flexibilidade do Abaré permite que a inclusão de serviços através do Agente Expansor.

Os testes de carga com o Agente de Coleta mostraram que o sistema pode suportar um numero de 40 requisições sem gerar sobrecarga no sistema. Já os testes com os Agentes Inteligentes comprovaram a viabilidade do Middrouter para prover inteligência e autonomia da rede.

Como trabalhos futuros, pretendemos ampliar os módulos já propostos incluindo módulos de gerenciamento de usuários, *Qualidade de Serviço* (QoS) e *Qualidade de Experiência* (QoE).

Agradecimentos

Este trabalho foi financiado pela FAPESPA, FADESP, PROPESP – UFPA e CNPq (476202/2009-4.)

Referências

Aggelou, G. Wireless Mesh Networking With 802.16, 802.11, and ZigBEE.2008.

Aguiar, E. ; Bittencourt, P. ; Moreira, W. ; Abelém, A . Estudo comparativo de protocolos de roteamento para redes Mesh na região Amazônica. In: 25º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, Belém/PA, Brazil. , 2007. v. 2. p. 1105-1110.

Berners-Lee,T. Fielding, R. e Frystyk, H., Hypertext Transfer Protocol - HTTP/1.0, RFC 1945, May 1996.

Campista, M. E. M. and at All, "Routing metrics and protocols for wireless mesh networks," Network, IEEE, vol. 22, no. 1, pp. 6–12, 2008.

Capone, A., Cesana, M., Napoli, S. e Pollastro, A. (2007) "MobiMESH: A Complete Solution for Wireless Mesh Networking", IEEE MASS 2007 (4th IEEE International Conference on Mobile Ad Hoc and Sensor Systems) Pisa, Italy.

Cisco, "Cisco mesh products", ultimo Acesso, Março 2010. Disponível: <http://www.cisco.com/en/US/products/ps8368/index.html>

DD-WRT, "DD-WRT", Disponivel em: <http://www.ddwrt>. ultimo acesso, Dezembro 2010.

IEEE , "Ieee draft p802.11s d4.0." IEEE Unapproved Draft Std P802.11s/D4.0, Março 2010.

Ito, M., Shikama, T., e Watanabe, A. 2009. Proposal and evaluation of multiple gateways distribution method for wireless mesh network. 3rd international Conference on Ubiquitous information Management and Communication.

Jardosh, A. P. Suwannatat, P. Hollerer, T. Belding E. M. , and Almeroth, K. C. , "Scuba: Focus and context for real-time mesh network health diagnosis." in PAM, ser. Lecture Notes in Computer Science, M. Claypool and S. Uhlig, Eds., vol. 4979. Springer, 2008, pp. 162–171.

Kephart, J. O. e Chess, D. M.The vision of autonomic computing. Computer, 36(1):41–50, 2003.

Khalid, A., Haye, M. A., Khan, M. J., and Shamail, S. 2009. Survey of Frameworks, Architectures and Techniques in Autonomic Computing.In Proceedings of the 2009 Fifth international Conference on Autonomic and Autonomous Systems.

Microsoft, "MCL.". Disponivel em, <http://research.microsoft.com/mesh/>, Acessado em Março de 2010.

Moreira, W.; Aguiar, E.; Abelém, A. J. G.; Stanton, M.Using Multiple Metrics with the Optimized Link State Routing Protocol fo Wireless Mesh Networks. 26° Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, SBRC 2008. Maio 2008.

Motorola, "MotoMesh", Acessado em Março de 2010. Disponível em http://developer.motorola.com/products/twowayradios/motomesh/ .

Nanda, S.e Kotz D. , "Mesh-mon: A multi-radio mesh monitoring and management system," Comput. Commun., vol. 31, no. 8, pp. 1588–1601, 2008.

Openwrt, "Openwrt wireless fredom," Disponivel em: <http://openwrt.org/> .Ultimo

acesso, Março 2010.

Park, N. e Lee, G. "Agent-based Web services middleware," Global Telecommunications Conference, 2003. GLOBECOM '03.IEEE , vol.6, no., pp. 3186-3190 vol.6, 1-5 2003.

Passos, D. e Albuquerque, C., “Uma Abordagem Unificada para Métricas de Roteamento e Adaptação Automática de Taxa em Redes em Malha Sem Fio”, *Simpósio Brasileiro de Redes de Computadores(SBRC 2009)*, Recife, maio de 2009.

Pinheiro, B. A. ; Nascimento, V. B. ; Moreira, W. ; Abelém, A . Abaré: A Deployment and Management Framework for Wireless Mesh Network. In: IEEE Latin-American Conference on Communications (IEEE LatinCom 2009), 2009, Medellín, Colombia.

Ramachandran, K. Belding-Royer E., e Aimeroth K., “Damon: a distributed architecture for monitoring multi-hop mobile networks,” Oct. 2004, pp. 601–609.

ReMesh, “ReMesh”. Disponivel em: <http://vmesh.inf.uth.gr/>.Ultimo acesso, Março 2010.

Riggio, R. Scalabrino, N. Miorandi, D. e Chlamtac, I. “Janus: A framework for distributed management of wireless mesh networks,” TridentCom 2007. 3rd International Conference on, 2007.

Tsarmpopoulos, N., Kalavros I. e Lalis S. (2005) A Low-cost and Simple-to-Deploy Peer-to-Peer Wireless Network based on Open Source Linux Routers.

Vmesh, “Vmesh - wireless network testbed”, Disponivel em: <http://vmesh.inf.uth.gr/>, ultimo acesso, Março 2010.

LiTE: Um Algoritmo de Localização Temporal e Ordenação de Eventos em Redes de Sensores Sem Fio Compostas por Nós Dessincronizados

Leonardo L. Guimarães[1], Horácio A.B.F. Oliveira[1], Rômulo T. Rodrigues[2], Edjair S. Mota[1], Antonio A.F. Loureiro[3]

[1]Depto. de Ciência da Computação – Universidade Federal do Amazonas, Brasil
[2]Depto. de Engenharia Electrotécnica e Computadores – Universidade do Porto, Portugal
[3]Depto. de Ciência da Computação – Universidade Federal de Minas Gerais, Brasil

{horacio,leonardo,edjair}@dcc.ufam.edu.br
ee09264@fe.up.pt, loureiro@dcc.ufmg.br

Abstract. *Wireless Sensor Networks are basically designed to monitor and detect events of interest. Two key aspects of this task are the identification of the exact time of occurrence of an event and, mainly, the ordering of several events in the network. Current solutions propose different algorithms for clock synchronization for sensor nodes. However, these solutions require constant executions to keep the network synchronized, since the sensor clocks quickly get unsynchronized (up to 3 seconds per day). In this work, we propose the LiTE algorithm, a novel, simple, and efficient algorithm for temporal localization and ordering of events in these networks. The proposed algorithm does not require clock synchronization of the sensor nodes. Laboratory experiments with real sensor nodes prove the applicability of the proposed algorithm and extensive simulation experiments show the scalability and efficiency of the proposed solution.*

Resumo. *Redes de Sensores Sem Fio são redes basicamente projetadas para monitorar e detectar eventos de interesse. Dois aspectos chaves desta tarefa são a identificação exata do tempo de ocorrência de um evento e, principalmente, a ordenação e o sequenciamento da ocorrência de diversos eventos na rede. Soluções atuais propõem diferentes algoritmos de sincronização de relógios dos nós sensores. Entretanto, tais soluções requerem constantes execuções para manter a rede sincronizada, já que os relógios dos sensores rapidamente se dessincronizam (até 3 segundos por dia). Este trabalho propõe o algoritmo LiTE, uma nova abordagem, simples e eficiente, para localização temporal e ordenação de eventos em tais redes, que não requer sincronização dos nós sensores. Experimentos práticos em laboratório com nós sensores reais comprovam a aplicabilidade do modelo e simulações extensivas mostram a escalabilidade e robustez da solução proposta.*

1. Introdução

Redes de Sensores Sem Fio (RSSFs) são compostas por nós sensores que cooperam entre si a fim de monitorar uma área de interesse comum [Akyildiz et al. 2002, Estrin et al. 2001, Loureiro et al. 2003]. Esta tecnologia pode ser empregada nas mais diversas situações: monitoração de ambientes inóspitos, instalações médicas, urbanas,

militares, industriais, etc. À medida que ocorrem avanços tecnológicos nas áreas de sensores, nanotecnologia, circuitos integrados e comunicação sem fio, a utilização das RSSFs nas mais diversas aplicações se torna uma possibilidade revolucionária, por se tratar de uma ferramenta de coleta e processamento de informação, que tende a ser escalável e de baixo custo.

Tais RSSFs são voltadas basicamente à detecção e monitoração de eventos. Eventos possuem duas características principais: a primeira é qualitativa (*critério causal*), diz respeito à variável monitorada (e.g., temperatura, luminosidade, som, pressão); a segunda característica é referente à localização, tanto espacial quanto temporal (*critério espaço-temporal*), e indica quando e onde um evento ocorreu [Oliveira et al. 2009, Davidson 1980]. Enquanto que o primeiro critério é facilmente identificado usando o dispositivo sensorial que o detectou, o critério espaço-temporal só pode ser identificado usando-se o posicionamento dos nós sensores e também, em geral, os seus relógios. Considerando que os nós sensores de uma RSSF são basicamente estáticos, o critério espacial, uma vez identificado, permanece o mesmo ao longo do tempo.

Entretanto, manter os relógios dos nós sensores sincronizados é um desafio muito grande uma vez que estes se dessincronizam a uma taxa de $40\,\mu s/s$ [Maroti et al. 2004]. A essa taxa de dessincronização, os nós sensores precisarão ser sincronizados a cada $25\,s$ para manter uma sincronização na faixa dos milissegundos. Tendo em vista esta problemática, diversos trabalhos propõem algoritmos de sincronização leves e passíveis de serem executados continuamente, dentre os quais podemos citar: *Reference Broadcast Synchronization* [Elson et al. 2002], *Flooding Time Synchronization Protocol* [Maroti et al. 2004], *Delay Measurement Time Synchronization* [Ping 2003] e *Post-Facto Synchronization* [Elson and Estrin 2001].

Neste trabalho, uma nova abordagem, simples e eficiente, para localização temporal e ordenação de eventos em RSSFs está sendo proposta. Nesta abordagem, implementada no algoritmo LiTE (Localização Temporal de Eventos), não se procura sincronizar os nós sensores entre si, mas sim sincronizar o evento com o relógio do nó sink, responsável por coletar e agregar todos os eventos da rede. Tal algoritmo se baseia no cálculo preciso dos atrasos dos pacotes enviados em múltiplos saltos a partir do nó que detectou o evento até o nó sink. Experimentos reais conduzidos em laboratório através de osciloscópios e nós sensores atestam a possibilidade do cálculo destes atrasos enquanto que simulações extensivas usando o simulador NS-2 demonstram a escalabilidade, a eficiência e a robustez da solução proposta.

O restante deste trabalho está organizado como segue. Soluções atuais encontradas na literatura são discutidas na seção 2. Na seção 3, são introduzidos alguns conceitos relevantes à compreensão deste trabalho. Em seguida, na seção 4, é apresentado o algoritmo proposto, o LiTE. Na seção 5, são feitas avaliações de aplicabilidade e de desempenho. Na seção 7, alguns aspectos sobre a aplicabilidade e possível substituição dos algoritmos atuais pelo proposto neste trabalho são discutidos. Por último, na seção 6, são apresentadas conclusões relativas aos resultados obtidos e possíveis aspectos que deverão ser tratados em trabalhos futuros.

2. Trabalhos Relacionados

O *Reference Broadcast Protocol* (RBS) [Elson et al. 2002] é um protocolo de sincronização que utiliza um *broadcast* de referência, o qual é originado a partir de nós especiais (*beacons*) que possuem o tempo de "referência". Os nós *beacons* realizam o *broadcast* de referência e, em seguida, seus nós vizinhos fazem um *broadcast* informando o tempo de recebimento deste pacote, possibilitando a criação de uma tabela com os atrasos (*offsets*) relativos à cada vizinho. Este algoritmo apresenta a vantagem de eliminar muitas fontes de erro no processo de sincronização. Entretanto, seu custo computacional é elevado se comparado com as demais soluções – $O(2 * n)$, onde n é a quantidade de nós na rede.

No protocolo *Flooding Time Synchronization Protocol* (FTSP) [Maroti et al. 2004], o nó sink (que possui o tempo de referência) faz um *broadcast* dando inicio ao *flooding* na rede. Os demais nós, ao receberem esse pacote, fazem um *timestamp* na camada MAC (*Media Access Control*), calculam os atrasos do tempo de transmissão em relação ao sink, e repassam o pacote com as devidas correções, dando continuidade ao *flooding*. Ao final, todos os nós alcançáveis da rede terão realizado um *broadcast* e toda a rede estará sincronizada com uma determinada precisão. O custo de comunicação do FTSP é de um pacote enviado por cada nó da rede – $O(n)$.

O *Delay Measurement Time Synchronization* (DMTS) [Ping 2003] pode ser utilizado para sincronização local (assim como o RBS), ou global (como o FTSP). A sincronização local ocorre como segue. Em uma determinada região é eleito um nó líder (referência), o qual faz um *broadcast* com o seu tempo. Ao contrário do RBS, os vizinhos não trocam pacotes entre si. Eles se sincronizam com o tempo do líder, calculando o *atraso de transmissão do pacote* (detalhado na seção 3). A sincronização por múltiplos saltos funciona da mesma forma, porém após cada vizinho se sincronizar, ele deve realizar um *broadcast* contendo o seu tempo sincronizado, ou seja, funciona como um algoritmo de inundação (*flooding*) com custo $O(n)$. Existe uma forte semelhança entre o DMTS e o FTSP, mas o que os difere é basicamente a forma de calcular o *atraso*.

O algoritmo *Post-Facto Synchronization* [Elson and Estrin 2001] é um algoritmo de sincronização instantânea voltada especificamente para eventos. Assim como o RBS, é necessário que hajam nós de referência espalhados ao longo da rede. No entanto, esses nós *beacons* só realizam o *broadcast* de referência caso algum vizinho detecte um evento e solicite o tempo real [Elson and Estrin 2001]. Desta forma há uma ordenação precisa dos eventos, porém se vários eventos são detectados praticamente todo o tempo, várias solicitações de sincronização serão realizadas.

Como pode-se observar, existem diferentes propostas buscando soluções cada vez mais eficientes na área de sincronização. Embora existam diversas vantagens na utilização de algoritmos de sincronização, é importante destacar que isto implica em consumo extra de energia da rede, que é escassa em RSSFs. Considerando que em nós sensores Mica2 há uma taxa de dessincronização de $40\,\mu s/s$ [Maroti et al. 2004], isso acarretará em uma dessincronização de aproximadamente $3,5s$ por dia e a rede precisará ser ressincronizada frequentemente, o que resulta em mais consumo de energia. Neste trabalho, uma nova abordagem está sendo proposta: não se preocupar com a sincronização dos nós sensores, mas sim dos eventos. Nesta abordagem, nenhum pacote será trocado para sincronizar nós com relação a alguma referência. Além disso, a sincronização do evento é realizada com

o próprio pacote que o nó sensor envia ao sink informando a respeito da ocorrência do evento, o que gera uma solução com custo de comunicação praticamente nulo.

3. Definição do Problema

Definição 1 (Rede de Sensores Sem Fio) *Uma RSSF pode ser representada formalmente como um grafo Euclidiano $G = (V, E)$ como segue:*

- $V = \{v_0, v_1, \ldots, v_{n-1}\}$ *é o conjunto de nós sensores (vértices do grafo), sendo que v_0 é o nó sink;*
- $\forall v_i \in V$, r *é o raio de comunicação de v_i;*
- $Q = [0, x] \times [0, y] \times [0, z]$ *a região de sensoriamento em três dimensões;*
- $\langle i, j \rangle \in E$ *se, e somente se, a distância entre v_i e v_j for menor que r, i.e., v_i alcança v_j e vice-versa;*
- t *é o tempo global da rede; pode ser baseado no UTC (Coordinated Universal Time, e.g., GPS) ou em um tempo relativo (e.g., do nó sink).*
- $\forall v_i \in V$, $t_i(t)$ *é o tempo local em que v_i se encontra no instante t.*

Conforme mencionado, redes de sensores são basicamente voltadas à monitoração, detecção e notificação de eventos.

Definição 2 (Eventos e Histórico Local e Global de Eventos) *Um evento pode ser definido como "algo que acontece em um dado lugar e tempo" ou "um fenômeno localizado em um único ponto do espaço-tempo" [Fellbaum 1998]. Do ponto de vista temporal em RSSFs, um evento pode ser detectado por um ou mais nós e pode ser definido como:*

- e_i^t *é o evento e sendo detectado pelo nó v_i no seu tempo local t_i;*
- $h_i = \{e_i^{t_1}, e_i^{t_2}, \ldots\}$ *é o histórico ordenado de eventos do nó v_i;*
- $\{h_1 \cup h_2 \ldots \cup h_n\} \rightsquigarrow H$ *é o histórico global de eventos ordenado pelo tempo global t;*

Em RSSFs, o *histórico local* pode ser facilmente calculado ordenando-se os eventos detectados usando os relógios locais dos nós sensores. Entretanto, para que esta informação seja útil, ela precisa ser convertida em um *histórico global* que é o histórico de todos os eventos da rede que, neste trabalho, é a definição de *ordenação de eventos* (figura 1):

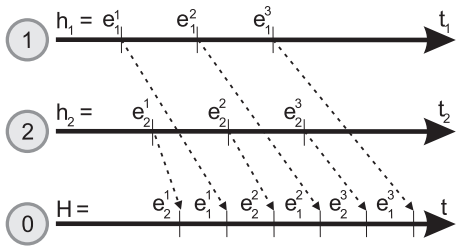


Figura 1. Ordenação de eventos.

Definição 3 (Ordenação de Eventos) *Conversão de $\{h_1 \cup h_2 \ldots \cup h_n\}$ em H.*

Uma solução para este problema de ordenação de eventos é manter todos os nós da RSSF sincronizados com o tempo global t:

Definição 4 (Sincronização de Nós e Erro de Sincronização) $\forall v_i \in V$ *atualizar $t_i(t) \approx t$. Diga-se aproximado, pois nenhum algoritmo de sincronização é perfeito por se basearem em técnicas que geram erros. O erro de sincronização de um nó i é definido como $t_i(t) - t$.*

Quando os nós sensores estão com seus relógios sincronizados, H é facilmente gerado ordenando-se os eventos por seus tempos locais t_i (que são aproximações do tempo global t). Em RSSFs, por seus protocolos serem baseados em múltiplos saltos, uma das técnicas comumente utilizadas em sincronização é a estimativa de atraso de um pacote em um salto (figura 2).

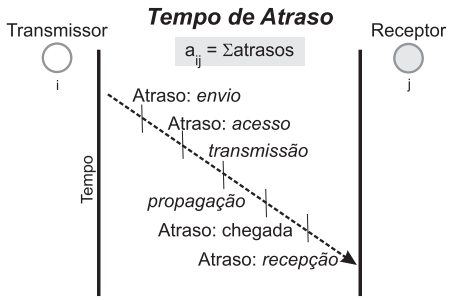


Figura 2. Atraso de um salto.

Definição 5 (Estimativa de Atraso de um Salto – a_{ij}^p)
Estimativa de atraso (delay measurement [Ping 2003, Oliveira et al. 2009]) consiste em calcular, ou estimar, todos os possíveis atrasos existentes durante a transferência de um pacote p, em um único salto, do nó transmissor i para o nó receptor j: $a_{ij}^p = a_{env}^p + a_{mac}^p + a_{trans}^p + a_{prop}^p + a_{cheg}^p + a_{recep}^p$, *onde:*

- a_{env}^p *é o atraso de envio*; onde ocorre a montagem da mensagem, e cabeçalho. Este atraso é variável e não determinístico pois o processo de envio concorre com outros processos e é dependente do sistema operacional;
- a_{mac}^p é o *atraso da camada MAC*; está diretamente relacionado ao estado do canal, ou seja, neste momento o nó está disputando com os demais sensores um momento para enviar seu pacote;
- a_{trans}^p *é o atraso de transmissão*; é determinístico, pois está relacionado ao tempo decorrido durante a transmissão bit a bit do pacote, dependendo principalmente do tamanho do pacote;
- a_{prop}^p *é o atraso de propagação*; dado que a velocidade de propagação de uma onda eletromagnética é de aproximadamente $3 \times 10^8\, m/s$, basta relacionar essa velocidade com o espaço percorrido;
- a_{cheg}^p *é o atraso de chegada*; tempo de recebimento do pacote completo; determinístico e depende do tamanho do pacote;
- a_{recep}^p *é o atraso de recepção*; tempo decorrido durante a montagem do pacote e interrupção do sistema operacional; este tempo varia dependendo do SO, portanto é um tempo não determinístico.

4. LiTE - Localização Temporal de Eventos

Nesta seção, é apresentado um novo algoritmo para sincronização e ordenação de eventos em RSSFs: o LiTE (Localização Temporal de Eventos).Conforme mencionado, o ponto chave do algoritmo LiTE está em reconhecer que manter nós sensores sincronizados gera um custo elevado para apenas determinar o tempo e ordem de ocorrência de eventos em uma RSSF. Desta forma, o algoritmo LiTE procura apenas sincronizar o tempo em que o evento foi detectado pelo nó sensor em relação ao tempo do nó sink. Para isso, o algoritmo consiste em calcular o *atraso de roteamento do pacote* (figura 3).

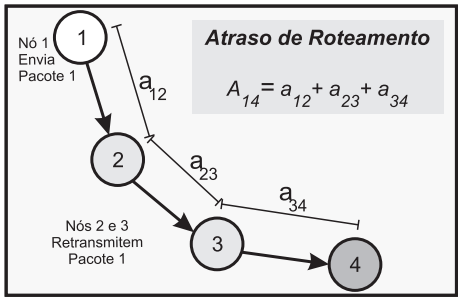


Figura 3. Atraso de roteamento.

Algoritmo 1 - LiTE

▷ **Entrada:**
1: Nó sensor v_i detecta o evento $e_i^{t_i}$.
Ação:
2: $tmEv_i \leftarrow t_i$; {Salva o tempo de detecção do evento}
3: $proxSalto_i \leftarrow calculaProxSalto()$; {Calcula o próximo salto em direção ao sink}
4: $A_i \leftarrow t_i - tmEv_i$; {Atualiza o atraso de roteamento}
5: Envia $pacote(e_i^{t_l}, A_i)$ para $proxSalto_i$. {Envia consulta para a rede}

▷ **Entrada:**
6: $msg_i = pacote(e_k^{t_k}, A_k)$ tal que $a_i = calculaAtrasoSalto(msg_i)$.
Ação:
7: **se** $i \neq 0$ **então** -{SE: este nó não for o sink ...}-
8: $tmPac_i \leftarrow t_i$; {Salva o tempo de chegada do pacote}
9: $proxSalto_i \leftarrow calculaProxSalto()$; {Calcula o próximo salto da resposta}
10: $A_i \leftarrow A_k + a_i + (t_i - tmPac_i)$; {Atualiza o atraso de roteamento}
11: Envia $pacote(e_i^{t_l}, A_i)$ para $proxSalto_i$. {Envia consulta para a rede}
12: **senão**
13: $A_i \leftarrow A_k + a_i$; {Atualiza o atraso de roteamento}
14: $t_k = t_i - A_i$; {Calcula o tempo global do evento}
15: $H \leftarrow H \cup \{e_k^{t_k}\}$; {Registra o evento no histórico global}
16: **fim se**

Definição 6 (Atraso de Roteamento do Pacote – A_{ij}^p) *Tempo total que o pacote p levou para deixar o nó v_i e chegar, em múltiplos saltos, ao nó v_j (em geral, o nó sink). Esse cálculo é possível somando-se todos os atrasos e todos os tempos de processamento dos nós intermediários (i.e., que repassaram o pacote) até o momento que este atingiu o nó de destino, conforme ilustrado na figura 3. Logo, $A_{ij}^p = a_{ik}^p + \ldots + a_{lj}^p$, onde $\{v_k, \ldots, v_l\}$ são nós intermediários que repassaram o pacote.*

O atraso de roteamento pode ser calculado usando qualquer protocolo de roteamento, uma vez que qualquer atraso introduzido pelo roteamento será calculado nesta fase do algoritmo LiTE. É importante ressaltar que tanto o processo de cálculo de atraso dos saltos quanto o de roteamento não requerem sincronização de relógios entre os nós sensores.

O algoritmo 1 descreve o funcionamento do algoritmo LiTE proposto neste trabalho. O algoritmo é simples e eficiente, e não requer nenhuma configuração inicial (i.e., troca de mensagens para sua configuração). Neste algoritmo, quando um determinado nó sensor detecta um evento (linha 1 do algoritmo 1), este irá registrar o tempo local de detecção do evento (linha 2) e, em seguida, irá solicitar ao protocolo de roteamento o próximo salto do pacote (linha 3). Como este último passo pode demorar dependendo do protocolo de roteamento (reativo, pró-ativo, híbrido), o atraso de roteamento é atualizado com este tempo de processamento local (linha 4). Em seguida, o nó encaminhará o pacote com o registro do evento para o próximo nó sensor em direção ao sink (linha 5).

Cada nó sensor intermediário irá calcular o atraso do salto ao receber o pacote (linha 6), registrar o tempo de recebimento do pacote (linha 8) e calcular o próximo salto do pacote (linha 9). Em seguida, o nó intermediário irá acrescentar ao atraso de roteamento do pacote o seu atraso de salto mais o seu tempo de processamento (linha 10) e, por último, encaminhar o pacote para o próximo salto (linha 11). Quando o pacote chegar

ao nó sink, este irá também calcular o atraso do salto e acrescentá-lo ao atraso de roteamento (linha 13). Por último, o nó sink irá calcular o tempo real de ocorrência do evento como sendo o tempo atual subtraído do atraso do pacote e, então, registrar o evento em sua ordem correta no histórico global de eventos.

A implementação do cálculo de atraso de um salto pode ser realizada apenas na camada de aplicação ou pode tirar proveito de informações de tempo introduzidas na camada MAC. Para isso, duas variações do LiTE foram implementadas: o *LiTE Apl*, implementado apenas na camada de aplicação (conforme o algoritmo apresentado), e o *LiTE Mac*, implementado introduzindo-se marcações de tempo na camada MAC.

No *LiTE Mac*, um código é introduzido logo após o nó sensor obter acesso livre ao meio e logo antes do pacote ir para o *driver* de rede para ser enviado (antes da camada física). Esse código obtém o atraso da camada de aplicação até o momento de acesso livre ao meio e adiciona esse atraso ao atraso de roteamento. Outro código no nó receptor é responsável por armazenar uma marcação de tempo no instante em que o *driver* de rede receber o pacote. Essa marcação de tempo, junto com o tempo de recebimento na aplicação, será adicionado ao atraso de roteamento. Nesta versão do LiTE, grande parte dos tempos não determinísticos de envio e recepção de pacotes podem ser eliminados, gerando um cálculo de atraso mais preciso.

5. Avaliação de Desempenho

Nesta seção, o desempenho do algoritmo LiTE será avaliado sob três aspectos: aplicabilidade, escalabilidade e robustez. O primeiro aspecto, experimentado em nós sensores reais, avalia a técnica de cálculo de atraso de um salto e é apresentado na seção a seguir.

5.1. Experimentos em Nós Sensores

O objetivo destes experimentos é analisar o impacto dos erros não determinísticos na técnica de cálculo de atrasos quando implementada em nós sensores reais, mais especificamente, nos nós sensores SunSPOT [SunLabs 2009]. Apesar de experimentos similares terem sido aplicados em outros trabalhos [Maroti et al. 2004], este é o primeiro a experimentar tal técnica em sensores SunSPOT e o primeiro a comparar dados obtidos tanto na camada MAC quanto na de Aplicação. Além disso, como será mostrado a seguir, resultados diferentes foram obtidos por tal técnica quando implementada nestes nós sensores.

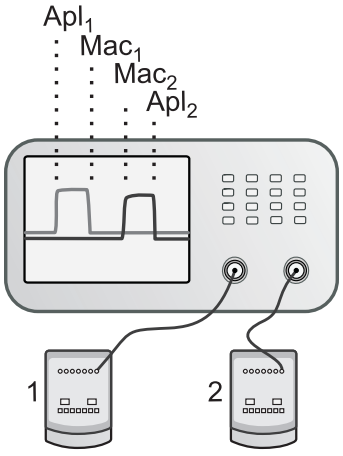


Figura 4. SunSPOTs.

5.1.1. Metodologia

Para calcular o tempo de envio e recepção de um pacote e, mais importante, calcular a variação deste tempo (tempos não determinísticos), um relógio externo, com tempo global, foi necessário. Para isso, dois nós sensores, um transmissor e um receptor, foram conectados a um osciloscópio de alta precisão (MS06032A, *Agilent Technologies*, com precisão de 25 μs – figura 4). Pacotes iguais com tamanho de 52 bytes são então enviados pelo transmissor. Na camada de aplicação antes de solicitar o envio do pacote, o sinal da

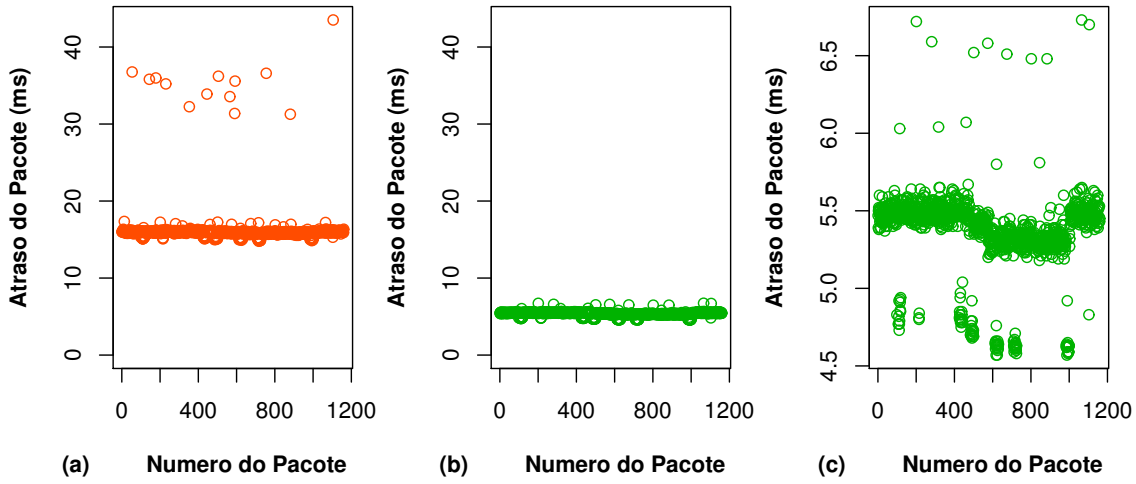


Figura 5. Atrasos dos pacotes na camada de aplicação (a); e MAC (b,c).

saída digital $D0$ sobe para nível lógico 1 (marcação Apl_1, da figura 4), permanecendo assim até que todas as verificações da disponibilidade do meio sejam feitas e, finalmente, o pacote esteja pronto para ser enviado, tornando ao nível lógico inicial 0 (marcação Mac_1). Após a chegada do pacote no receptor (atraso de chegada), o nível lógico da saída digital D0 deste nó sobe para 1 (marcação Mac_2) permanecendo assim até que, na aplicação, após a finalização do processo de recebimento do pacote, o nível volte ao seu valor inicial 0 (marcação Apl_2). Para cada pacote enviado e recebido, pode-se calcular o tempo de um salto tanto na camada de aplicação ($atrasoApl = Apl_2 - Apl_1$) quanto de acesso ao meio ($atrasoMac = Mac_2 - Mac_1$).

É importante notar que, neste experimento, não se procura calcular todos os atrasos do pacote, mas sim identificar atrasos não determinísticos, ou seja, os que variam inesperadamente de um pacote para outro, uma vez que tais atrasos não determinísticos são os responsáveis pela imprecisão da técnica.

5.1.2. Análise dos Resultados

Os gráficos da figura 5 ilustram os atrasos obtidos por diversos pacotes em um salto. Como pode-se observar na figura 5(a), mesmo sem concorrência de acesso ao meio, ainda assim alguns pacotes obtiveram atrasos bem maiores do que a média, indicando uma variação grande dos atrasos quando esta técnica é implementada na camada de aplicação. As figuras 5(a) e (b) ilustram os atrasos obtidos na camada MAC, sendo que esta última com uma visão mais detalhada. Como pode ser observado, tais atrasos variam cerca de $1\,ms$, principalmente abaixo da média.

Nas figuras 6(a,b), são mostrados os histogramas de densidade dos atrasos na camada de aplicação e MAC, respectivamente. Observando os gráficos, pode-se notar que, nestes sensores SunSPOT, os atrasos não seguem uma distribuição Gaussiana, conforme considerado por grande parte dos trabalhos que simulam algoritmos de sincronização. Isso é uma observação muito importante, pois a utilização de modelos errados pode gerar conclusões incorretas a respeito da eficiência dos algoritmos propostos. Para confirmar tal observação, os gráficos quantil-quantil da figura 7 comparam os quantis amostrais com os teóricos, indicando mais uma vez a não-normalidade dos dados pois vários pontos não estão próximos à reta de mínimos quadrados plotada.

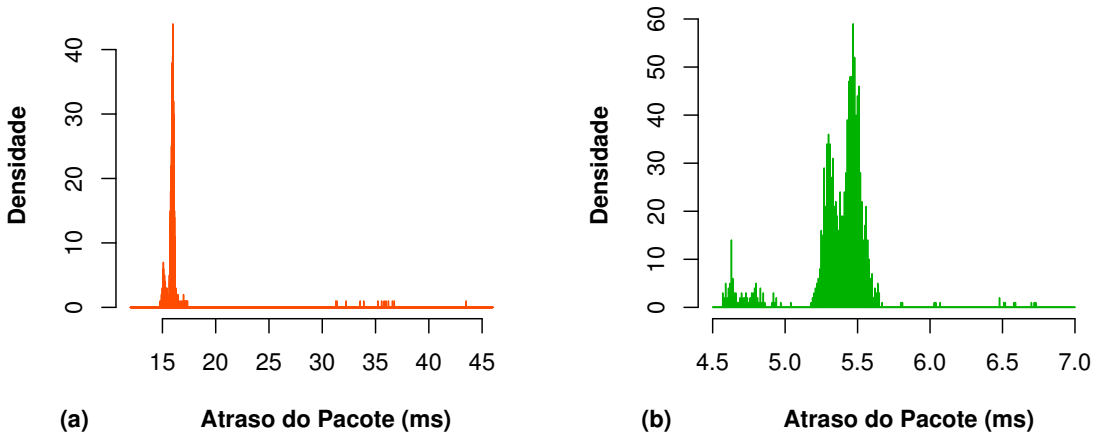


Figura 6. Histograma de densidade dos pacotes: aplicação (a); e MAC (b).

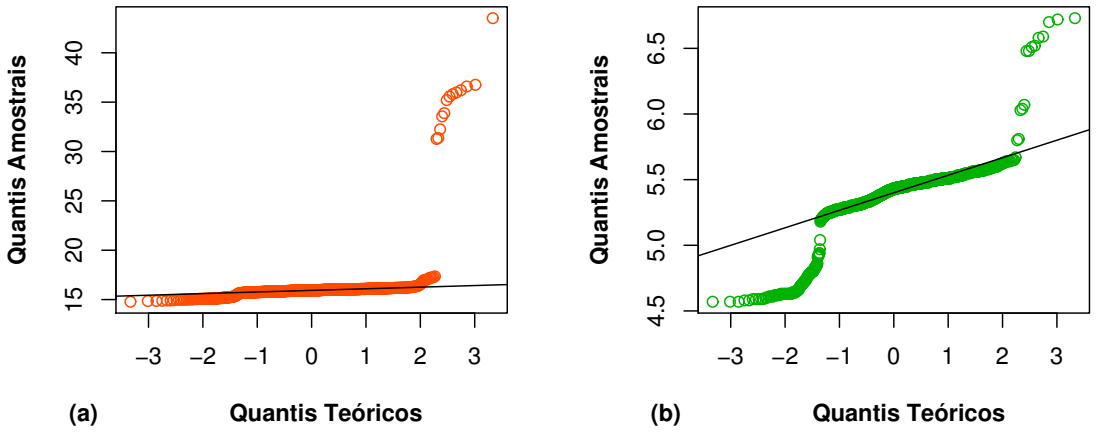


Figura 7. Quantis amostrais e teóricos dos atrasos: aplicação (a); e MAC (b).

Os gráficos Q-Q, apesar de serem bastante poderosos para verificar desvios de normalidade, não constituem um teste formal, servindo apenas para uma análise exploratória dos dados. Testes de adequação formais, tais como o *Chi-quadrado* e *Kolmogorov-Smirnov*, permitem uma análise mais profunda da questão. Desta forma, tais testes foram aplicados para um nível de confiança de 95% nos dados obtidos na camada de aplicação e na camada MAC e indicaram valor de prova $p\text{-}value < 0.01$ para ambos os testes. Esse $p\text{-}value$ é a medida do grau de concordância entre os dados e a hipótese nula H0 (no caso, que a distribuição de probabilidade dos dados é normal). Quanto menor o $p\text{-}value$, mais forte é a evidência contra H0. Uma regra prática de decisão é rejeitar a hipótese nula se $p\text{-}value \leq \alpha$, onde α é a taxa de erro. Como está-se procurando uma margem de confiança de 95%, então, $\alpha = 1 - 0.95 = 0.05$. Logo, com base nos testes aplicados com os dados coletados nas medições, deve-se rejeitar a hipótese de normalidade.

Do ponto de vista de aplicabilidade, pode-se observar pelos gráficos mostrados que os atrasos não determinísticos geram um erro de aproximadamente $1\,ms$ ao ser utilizar a camada MAC e um erro de aproximadamente $5\,ms$ na camada de aplicação. Uma vez que observa-se pouca variação nos atrasos, pode-se concluir que a técnica é passível de ser implementada em nós sensores reais e, mais especificamente, nos nós sensores SunSPOT.

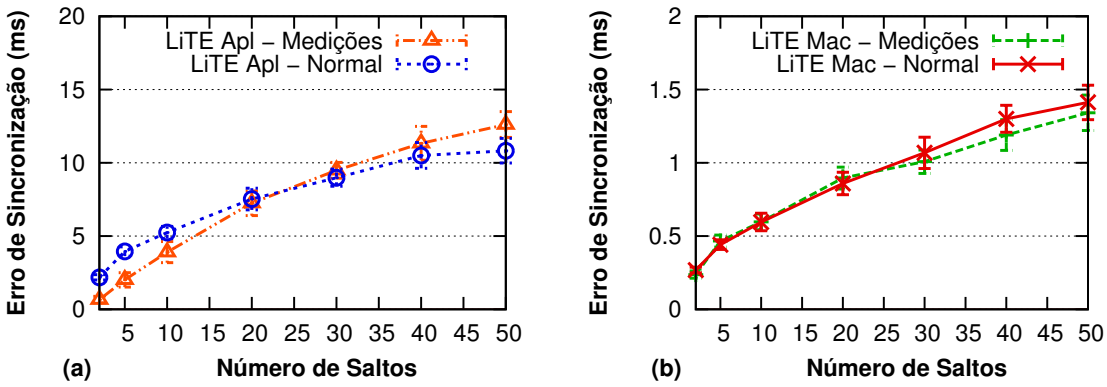


Figura 8. Erro de sincronização por número de saltos: aplicação (a); e MAC (b).

5.2. Experimentos de Escalabilidade e Robustez

O objetivo destes experimentos é avaliar o comportamento do algoritmo quando executado em múltiplos saltos em uma RSSF.

5.2.1. Metodologia

A avaliação de desempenho foi realizada utilizando o *Network Simulator 2* [McCanne and Floyd 2005]. Em todos os resultados, as curvas representam uma média das execuções, enquanto que as barras de erro, o intervalo de confiança para 95% de confiança a partir de 33 execuções diferentes (sementes aleatórias).

A tabela 1 apresenta valores padrões para os parâmetros de simulação. Os nós sensores são distribuídos no campo de monitoramento de acordo com uma grade perturbada, i.e., os nós tendem a ocupar a área uniformemente, mas sem formar uma grade regular. Para simular os erros de cálculo de atraso de um salto, foram utilizadas *simulações baseadas em medições* [Kashyap et al. 2008]. Nestas simulações, medições reais obtidas experimentalmente (neste caso, os atrasos calculados na seção anterior) são alimentadas ao simulador que irá utilizá-los quando necessário. Nesta abordagem não se tem os erros estatísticos observados ao se utilizar um modelo probabilístico.

Parâmetro	*Valor*
Campo de sensores	758 m × 758 m
Numero de nós	576 nós
Densidade	0.001 nós/m^2
Raio de comunicação	50 m
Atraso de um pacote	Medições
Erro de atraso	Medições

Tabela 1. Valores

5.2.2. Análise dos Resultados

Em termos de escalabilidade, o principal fator que afeta o algoritmo LiTE é a quantidade de saltos que o pacote percorre saindo do nó sensor que detecta o evento até o nó sink. Os gráficos da figura 8 mostram este impacto que a quantidade de saltos que o pacote percorre tem sobre o erro de cálculo de atraso e, consequentemente, na sincronização do evento. Como pode-se observar, os erros obtidos quando o algoritmo LiTE é implementado na camada de aplicação (figura 8(a)) são maiores e crescem mais rapidamente com o aumento do número de saltos do que quando implementado na camada de acesso ao

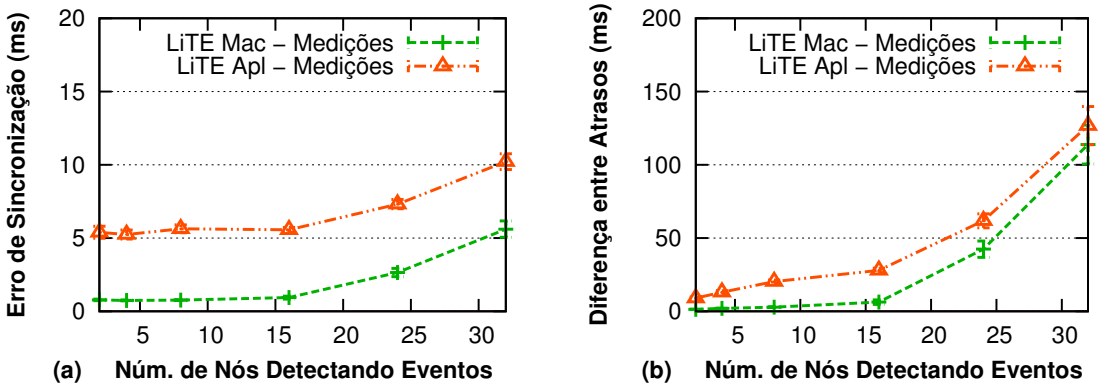


Figura 9. (a) Erro e (b) diferença de sincronização de eventos simultâneos.

meio (figura 8(b)). Uma outra observação importante é o erro de apenas 1.5 ms após 50 saltos quando o LiTE é implementado na camada MAC. Isso se deve ao fato do erro de cálculo de atraso de um salto poder ser anulado pelo erro de cálculo de atraso do salto seguinte. Ainda nesses gráficos, estamos comparando os resultados obtidos experimentalmente com a simulação dos erros usando uma distribuição normal. Pode-se observar uma certa diferença entre os resultados, em especial quando nos dados obtidos pela camada de aplicação. Nos gráficos seguintes, apenas as simulações baseadas em medições serão apresentadas.

Nos gráficos da figura 9, está-se avaliando a robustez do algoritmo para sincronizar eventos quando diversos eventos são detectados na rede. Para isso, diversos nós na rede, escolhidos aleatoriamente, detectaram um evento exatamente no mesmo instante. O gráfico da figura 9(a) mostra o comportamento do erro de sincronização dos eventos quando estes chegam no nó sink, enquanto que o gráfico da figura 9(b) mostra a diferença entre o menor e o maior tempo estimado do evento. Pode-se observar que em ambos os casos, o erro de sincronização dos eventos começa a crescer quando muitos eventos são detectados ao mesmo tempo, devido a atrasos maiores no envio e encaminhamento dos pacotes.

Foi avaliado também a capacidade do algoritmo LiTE de ordenar eventos na rede. Para isso, nos gráficos das figuras 10(a,b), 10 eventos foram gerados em ordem e em intervalos de tempo iguais (eixo X). Tais eventos foram então sincronizados no sink e ordenados usando o *LiTE Apl*, *LiTE Mac* e também usando a ordem de chegada dos pacotes no sink como a ordem dos eventos. Dois cenários foram avaliados. No primeiro cenário (figura 10(a)), os eventos estão próximos um do outro (e.g., um som alto sendo detectado por diversos sensores) e, no segundo cenário (figura 10(b)) os eventos estão espalhados aleatoriamente na rede (e.g., animais se movimentado em diversas partes). Como pode ser observado nos dois gráficos, o algoritmo *LiTE Mac* é capaz de acertar 100% da ordem dos eventos quando o tempo entre estes é maior do que $5\,ms$, mesmo no caso em que os eventos se encontram espalhados pela rede. Pode-se observar ainda, pelos gráficos, que a ordem de chegada dos pacotes no sink não e uma boa fonte de referência, principalmente no segundo cenário.

Por último, foi avaliada a capacidade do algoritmo LiTE de ordenar eventos à medida que a quantidade destes aumenta e mantendo-se o tempo entre eventos fixado

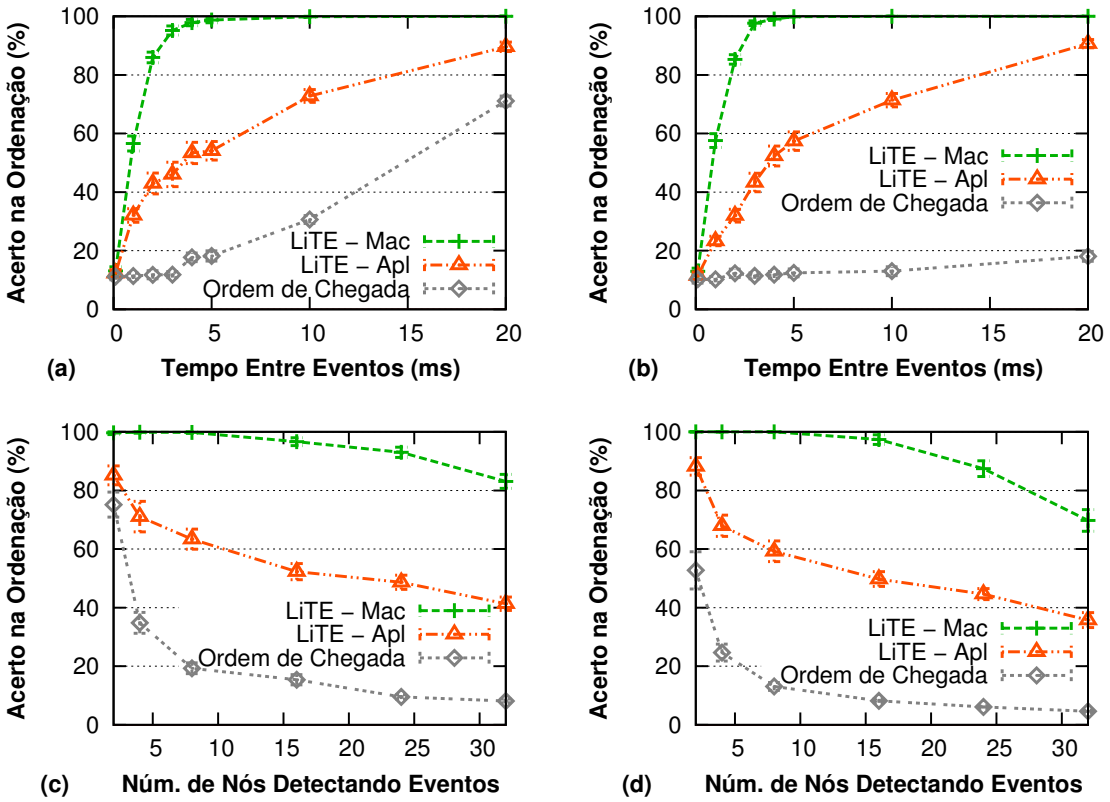


Figura 10. Acerto na ordenação de eventos próximos (a) e aleatórios (b).

em $5\,ms$ (figuras 10(c,d)). Novamente, foi-se avaliado o cenário em que eventos estão próximos (figura 10(c)) e espalhados (figura 10(d)). Pode-se observar que o algoritmo *LiTE Mac* foi capaz de ordenar corretamente mais de 90% de 20 eventos que estavam separados por apenas $5\,ms$ de tempo. Além disso, observa-se um comportamento com queda bem mais lenta da precisão deste último algoritmo em relação ao algoritmo *LiTE Apl* e na ordem de chegada dos pacotes no nó sink.

6. Aplicabilidade e Extensibilidade da Solução Proposta

Os resultados obtidos, em especial pelo algoritmo *LiTE Mac*, indicam que o mesmo é capaz de sincronizar e ordenar diversos eventos separados entre si por apenas $5\,ms$. Nesta precisão, uma aplicação poderia, por exemplo, identificar facilmente a localização de um som que estivesse a uma distância de pouco mais que $1.7\,m$ dos sensores.

A solução proposta no algoritmo *LiTE* pode ser facilmente utilizada nas mais diversas aplicações dos algoritmos de sincronização tradicionais sem a necessidade de modificação:

- *localização temporal de eventos*;
- *ordenação temporal de eventos*;
- *rastreamento de objetos*;
- *localização de sons*;
- *geração de mapas de energia*; etc.

Em outros casos, o algoritmo *LiTE* pode ser facilmente estendido para ser utilizado em algoritmos que precisam de processamento temporal distribuído como:

- *fusão de dados*: para combinar dados relacionados no tempo, cada nó intermediário pode sincronizar os eventos que este for combinar/encaminhar usando a mesma técnica executada pelo nó sink no algoritmo LiTE;
- *localização de sons e rastreamento* in site: nós vizinhos podem trocar pacotes com seus tempos locais e usarem o atraso do pacote para sincronizar seus relógios. Após o processamento distribuído, o dado processado poderá ser sincronizado globalmente no sink.

Além disso, o algoritmo *LiTE* não precisa se preocupar com questões como re-sincronização de nós devido ao *drift*, nós em modo *sleep*, tempo de convergência, complexidade computacional, tolerância a falhas, dentre outros; problemas estes que afetam todos os algoritmos de sincronização (apesar de poucos trabalhos levarem em consideração todos ao mesmo tempo).

7. Conclusão

Este trabalho propôs uma nova abordagem para o problema de sincronização e ordenação de eventos em RSSFs: o algoritmo LiTE – Localização Temporal de Eventos em RSSFs. Foi mostrado que, em muitos cenários, sincronizar todos os relógios da rede não apenas é um processo custoso como também desnecessário. Para solucionar tal problema, o algoritmo LiTE propõe a sincronização apenas dos eventos, e não dos nós sensores.

O desempenho do algoritmo LiTE foi avaliado tanto em experimentos práticos, em laboratório com nós sensores reais, que comprovaram a aplicabilidade do modelo, como também foi avaliado em simulações, mostrando a escalabilidade e robustez da solução proposta. O algoritmo *LiTE Mac* obteve o melhor desempenho nos experimentos realizados, tanto práticos quando simulados, e foi capaz de sincronizar eventos a 16 saltos de distância com erros próximos a apenas $1\,ms$ e foi capaz ainda de ordenar corretamente vários eventos espalhados pela rede e distantes apenas $5\,ms$ no tempo uns do outros. Pode-se dizer que o custo de comunicação do algoritmo é nulo, pois ele não requer troca de pacotes para configuração, aproveitando os pacotes utilizados no roteamento dos dados para o sink para enviar os dados de sincronização.

Os resultados obtidos são promissores. Algumas vantagens e limitações serão exploradas em trabalhos futuros como, por exemplo, identificar claramente quais os procedimentos que geram erros não determinísticos nos sensores e, então, modificá-los para reduzir tais atrasos e adaptá-los a uma rede que requer sincronização de eventos, uma vez que a implementação dos sensores atuais não levam isso em consideração. Pretende-se ainda implementar a técnica proposta em algoritmos de fusão de dados que necessitam de informações temporais.

Referências

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cyirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422.

Davidson, D. (1980). *Essays on Actions and Events*. Clarendon, Oxford.

Elson, J. and Estrin, D. (2001). Time synchronization for wireless sensor networks. In *IPDPS'01: Proceedings of the 15th International Parallel & Distributed Processing Symposium*, pages 1965–1970, Washington, DC, USA. IEEE Computer Society.

Elson, J., Girod, L., and Estrin, D. (2002). Fine-grained network time synchronization using reference broadcasts. *SIGOPS Operating Systems Review*, 36(SI):147–163.

Estrin, D., Girod, L., Pottie, G., and Srivastava, M. (2001). Instrumenting the world with wireless sensor networks. In *ICASSP'01: Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, pages 2033–2036, Salt Lake City, Utah.

Fellbaum, C. (1998). *Wordnet: An Electronic Lexical Database*. Bradford Books, 01 edition.

Kashyap, A., Ganguly, S., and Das, S. R. (2008). Measurement-based approaches for accurate simulation of 802.11-based wireless networks. In *MSWiM '08: Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 54–59, New York, NY, USA. ACM.

Loureiro, A. A. F., Nogueira, J. M. S., Ruiz, L. B., Mini, R. A. F., Nakamura, E. F., and Figueiredo, M. S. (2003). Redes de sensores sem fio. *SBRC'03: Proceedings of the 21st Brazilian Symposium on Computer Networks*, pages 179–226. Belo Horizonte, MG, Brasil.

Maroti, M., Kusy, B., Simon, G., and Ledeczi, A. (2004). The flooding time synchronization protocol. In *SenSys'04: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pages 39–49, Baltimore, MD, USA. ACM Press.

McCanne, S. and Floyd, S. (2005). ns network simulator. [Online] Available: http://www.isi.edu/nsnam/ns/.

Oliveira, H. A. B. F., Boukerche, A., Nakamura, E. F., and Loureiro, A. A. (2009). Localization in time and space for wireless sensor networks: An efficient and lightweight algorithm. *Performance Evaluation*, 66(3-5):209–222.

Ping, S. (2003). Delay measurement time synchronization for wireless sensor networks. Technical Report IRB-TR-03-013, Intel Research.

SunLabs (2009). Sun small programmable object technology (sun spot) developer's guide. [Online] Available: http://www.sunspotworld.com.

Maximização da vida útil de redes de sensores sem fio utilizando fusão de dados e roteamento *fuzzy*

Rafael Lopes Gomes[1], **Thiego Nunes**[1], **Dionne Monteiro**[1], **Antônio Gomes Abelém**[1]

[1]Faculdade de Computação – Universidade Federal do Pará (UFPA)
Rua Augusto Corrêa 01, 66075-110, Belém, PA, Brasil

Abstract. *Wireless Sensor Networks (WSN) are resource constraints networks, therefore the usage of protocols of Ad Hoc networks makes WSNs out of optimum performance. Within this context, this paper presents an extension of the Ad hoc On-demand Distance Vector (AODV) protocol that uses the techniques of data fusion across the network, fuzzy logic and transmission of informations through bursts to increase efficiency of energy consumption of sensors. The proposed extension, AODV - Fuzzy for Wireless Sensor Networks (AODV-FWSN), is evaluated in Network Simulator (NS-2). The simulations show that the proposed extension increases the lifetime of the network, maintaining the delivery efficiency of informations.*

Resumo. *As Redes de Sensores Sem Fio (RSSF) são redes que possuem restrições de recursos, sendo assim o uso dos protocolos das redes Ad Hoc faz com que as RSSFs não consigam obter um desempenho ótimo. Dentro desde contexto, este artigo apresenta uma extensão do protocolo Ad hoc On-demand Distance Vector (AODV) que utiliza as técnicas de fusão de dados ao longo da rede, lógica fuzzy e envio das informações através de rajadas para aumentar a eficiência do consumo de energia dos sensores. A extensão proposta, AODV – Fuzzy for Wireless Sensor Networks (AODV-FWSN), é avaliada no Network Simulator (NS-2). As simulações mostram que a extensão proposta aumenta a vida útil da rede mantendo a eficiência na entrega das informações.*

1. Introdução

Através da evolução das redes de sensores sem fio e do desenvolvimento de tecnologias como microprocessadores, comunicação sem fio, e micro sistemas eletro-eletrônicos [Akyildiz et al. 2002], uma rede pode monitorar e eventualmente controlar um ambiente.

As redes de sensores sem fio (RSSF) são compostas por pequenos dispositivos chamados nós sensores, onde os principais componentes do nó sensor são: bateria, o processador, a memória, o transceptor (responsável pela comunicação sem fio) e a unidade de sensoriamento.

Os nós da rede atuam de forma cooperativa disseminando uma determinada informação entre os outros nós até que os dados coletados alcancem um ponto de saída e possam ser processados pela aplicação cliente, este ponto de saída é denominado nó coordenador.

Há diversas aplicações para as RSSF sendo as principais relacionadas à pecuária, agricultura e ao meio ambiente. Um exemplo de aplicação é o monitoramento do microclima, onde sensores de monitoramento de temperatura e umidade estariam enviando dados da área monitorada para a estação base.

As redes de sensores sem fio diferem das redes tradicionais em muitos aspectos [Akyildiz et al. 2002]: não apresentam infra-estrutura nem ponto de acesso, apresentam diferentes consumos de energia, baixa capacidade de processamento e armazenamento, e isso infere diretamente nas características dos protocolos de roteamento.

Os protocolos de roteamento de redes convencionais e das redes Ad Hoc não se ajustam adequadamente às RSSF [Akkaya and Younis 2005], pois os nós sensores precisam de mecanismos de roteamento de forma que seu desempenho seja maximizado, tanto no processamento quanto na manutenção da energia, com isso quanto menor o consumo de energia maior será o tempo de vida de um nó em uma rede isolada.

As principais limitações das RSSFs são a diminuta quantidade de energia e de baixo processamento, devido a isso o tempo de vida da RSSF deve ser o maior possível para minimizar o custo de manutenção da rede.

Levando em consideração as limitações das RSSFs, o objetivo deste trabalho é customizar o protocolo de roteamento *Ad hoc On-demand Distance Vector* (AODV) [Perkins et al. 2002], afim de melhor adaptá-lo as RSSF e com isso garantir uma transmissão de dados mais eficaz e com menor consumo de energia.

Esta customização baseia-se nos princípios de fusão de dados ao longo da rede, lógica *fuzzy* e envio das informações através de rajadas. O objetivo com a utilização destas técnicas é fazer com que a rede proporcione um roteamento que maximize a fusão de dados e minimize o consumo de energia dos nós, garantindo uma maior longevidade para a rede. A proposta deste artigo é intitulada AODV – *Fuzzy for Wireless Sensor Networks* (AODV-FWSN).

O artigo esta organizado da seguinte forma: a Seção 2 mostra os trabalhos relacionados, a Seção 3 descreve o protocolo AODV, a seção 4 mostra o protocolo proposto AODV-FWSN, a Seção 5 descreve a avaliação da proposta e, finalmente, a Seção trata das conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Esta seção tem por objetivo mostrar trabalhos que propõem melhorias para as RSSF sobre vários aspectos, como: fusão de dados, maior eficiência no consumo de energia e na transmissão de dados multimídia, dentre outros aspectos.

Ding [Ding et al. 2004] desenvolve uma abordagem para manter a energia da rede equivalente e maximizar a vida útil desta. Esta abordagem enfatiza a manutenção de rotas, fazendo com que nós não críticos passem a ser usados como rotas, evitando gargalos na rede.

Kalantari [Kalantari and Shayman 2004] propõe encontrar rotas eficientes energeticamente, para isto ele usa um conjunto de equações diferenciais parciais semelhantes às equações de Maxwell na teoria eletrostática. Estas equações diferenciais parciais dão os caminhos de cada sensor para o nó central (coordenador).

Zhu [Zhu et al. 2009] propôs uma modelo matemático de otimização do tempo de vida para RSSFs, visando não só garantir a comunicação confiável, mas também de equilíbrio de carga da rede, e prolongar a vida útil das redes. Contudo, não leva em consideração a fusão de dados.

Salustiano [Salustiano et al. 2007] desenvolve um sistema para monitorar alguns ambientes remotos capaz de receber, processar e armazenar dados enviados pelos sensores, aplicando algoritmos para fundir dados de sensores.

A. R. Pinto [Pinto et al. 2007] cria um modelo de fusão de dados para RSSF afim de detectar intrusos, para isso o nó coordenador recebe os dados coletados e monitora o ambiente a partir destas informações. Entretanto, este não apresentou resultados sobre eficiência energética e a fusão de dados só acontece no coordenador.

Em nenhum dos trabalhos anteriormente citados encontra-se uma proposta que tenha como objetivo prover roteamento que melhore o consumo de energia e maximize a fusão de dados na rede simultaneamente.

3. Protocolo Ad hoc On-demand Distance Vector

O AODV é um protocolo de roteamento reativo para redes Ad Hoc móveis, ou seja, as tabelas de roteamento são preenchidas durante as operações de descoberta de rota.

O objetivo principal do protocolo é adaptar-se rápida e dinamicamente às variações das condições dos enlaces da rede, descobrindo rotas de forma a se evitar o desperdício de banda e minimizar o uso de memória e processamento nos nós.

A descoberta de rotas é feita através de trocas de mensagens de requisição de rota (*Route Request* - RREQ), resposta a requisição de rota (*Route Reply* - RREP) e aviso de queda de enlace (*Route Error* – RERR).

Quando um nó deseja enviar um pacote a outro nó, mas não há rota conhecida, este envia uma mensagem RREQ via *broadcast* à seus vizinhos, caso estes não possuam uma rota para o destino, prosseguem com a inundação da rede enviando RREQ aos seus demais vizinhos até que se chegue ao destino procurado, obtendo assim a rota para o destino e a rota reversa para o envio do RREP [Perkins et al. 2002].

O RREP é enviado via *unicast* para origem, uma vez que enquanto a requisição foi sendo propagada pela rede, caminhos reversos de todos os nós alcançáveis pela requisição até a origem vão sendo armazenados [Perkins et al. 2002].

4. AODV – Fuzzy for Wireless Sensor Networks

A extensão proposta para o protocolo AODV tem como objetivo prover um roteamento que maximize a fusão dos dados da rede e que prolongue a vida da mesma. Para isso, o protocolo proposto se baseia em três características principais:

- Sistema *Fuzzy*: gera-se um custo *fuzzy* para cada nó, onde este custo é utilizado como métrica para roteamento;
- Principio de Comutação em Rajadas: cada nó envia periodicamente uma rajada com os dados para o coordenador;
- Fusão dos Dados: os dados oriundos de outros sensores são incorporados à rajada do sensor atual.

Determina-se um custo, o *fuzzy cost* (FC), para cada nó, baseado nos valores de energia e grau de adjacência do nó, sendo que este grau de adjacência é o número de vizinhos diretos que o nó tem.

As informações de energia e grau de adjacência do nó são incorporadas às mensagens REPLY do protocolo AODV [Perkins et al. 2002], sendo assim o nó que requisitou a rota, recebe os FCs dos caminhos até o nó destino. Para isso cada nó que retransmite uma mensagem REPLY soma ao FC contido na mensagem o seu próprio FC.

A partir desse FC será possível escolher rotas em que a chance de fusão dos dados seja maior, visto que serão escolhidos os nós com grande adjacência, e que este nó não seja mais utilizado quando a sua energia se tornar crítica.

Com isso esperasse aumentar a vida da rede como um todo, fazendo com que o número de transmissões dos nós diminua e consequentemente a energia dos sensores se prolongue. A seguir será mostrado o sistema *fuzzy* desenvolvido e posteriormente o esquema de fusão de dados proposto.

4.1. Sistema Fuzzy Desenvolvido

A idéia de conjuntos *fuzzy* é uma extensão do conceito tradicional de conjuntos (*crisp*), onde um elemento pertence totalmente ou não a certo conjunto. Os conjuntos *fuzzy*, ao contrário, são definidos a partir de funções de pertinência cujo alcance é limitado a um intervalo entre 0 e 1. Ou seja, um valor entre 0 e 1 expressa o grau de pertinência de um elemento do conjunto *fuzzy* baseado nas inferências utilizadas. Normalmente, o grau de pertinência de um valor "x" em relação a uma função é representado por μ(x) [Adeli and Sarma 2006] [Zadeh 1965].

A seguir são mostradas as características do sistema *fuzzy* utilizado na proposta deste trabalho: funções de pertinência, o modelo de inferência, conjunto de regras e estratégia de defuzzificação considerados para a implementação da proposta.

4.1.1. Fuzzificação

O processo de fuzzificação tem como entrada os valores de energia e grau de adjacência do nó, sendo assim, são utilizadas duas funções de pertinência, as quais servem de entrada para o sistema *fuzzy*. O sistema *fuzzy* proposto utilizou funções triangulares e funções trapezoidais.

Uma função triangular possui três parâmetros: a, b e m. Sendo "a" o primeiro ponto e "b" o último ponto onde μ(x) é zero e "m" o ponto onde μ(x) possui valor 1. O grau de pertinência de uma função triangular é dado por [Adeli and Sarma 2006]:

$$\mu\left(x\right) = \begin{cases} 0 \;\; se\; x \;\leq\; a \\ \left(x-a\right) / \left(m-a\right) \;\; se\; x \;\epsilon\; [a,m] \\ \left(b-x\right) / \left(b-m\right) \;\; se\; x \;\epsilon\; [m,b] \\ 0 \;\; se\; x \geq b \end{cases}$$

A função trapezoidal tem 4 parâmetros: a, b, m1 e m2. Sendo "a" é o primeiro ponto e "b" o último ponto onde μ(x) é zero, os parâmetros "m1" e "m2" representam o intervalo de pontos onde μ(x) possui valor 1, ou seja, se x ϵ [m1,m2] $\Rightarrow$ μ(x) = 1. O grau de pertinência de uma função trapezoidal é determinado por [Adeli and Sarma 2006]:

$$\mu(x) = \begin{cases} 0 \;\; se\; x \;\leq\; a \\ (x-a)\,/\,(m-a) \;\; se\; x \;\epsilon\; [a, m1] \\ 1 \;\; se\; x \;\epsilon\; [m1, m2] \\ (b-x)\,/\,(b-m) \;\; se\; x \;\epsilon\; [m2, b] \\ 0 \;\; se\; x \geq b \end{cases}$$

A função de pertinência utilizada para os valores de energia recebidos é mostrada na Figura 1, possuindo três variáveis linguísticas, sendo definidas a partir de funções trapezoidais: *high*, *average* e *low*.

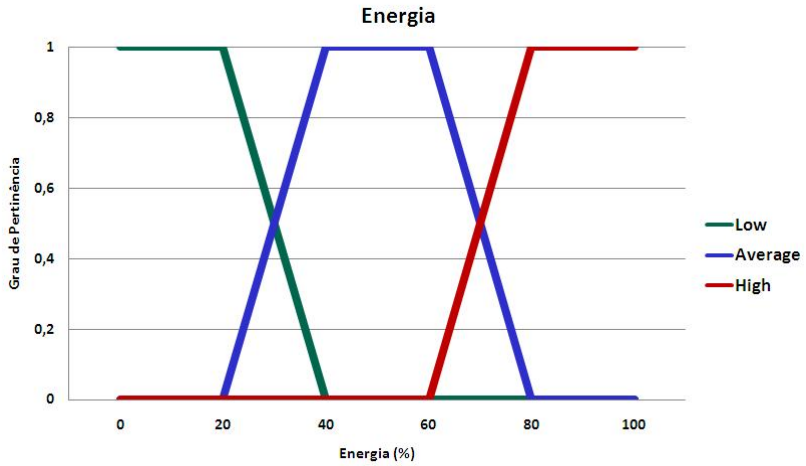


Figura 1. Função de Energia

Os valores energia que servem como entrada para a função são expressos em porcentagem. Esta função foi definida com o intuito de torná-la o mais genérica e abrangente, já que o valor numérico de medida de energia de cada sensor pode variar em função do modelo do sensor.

A função de pertinência utilizada para os valores de grau de adjacência do nó é mostrada na Figura 2, possuindo três variáveis linguísticas, sendo definidas a partir de três funções trapezoidais: *high*, *average* e *low*.

Os valores de grau de adjacência do nó representam o número de nós vizinhos diretos (adjacentes) ao nó em questão. O grau de pertinência máximo para a função "*High*" ocorre no intervalo de 7 a infinito, sendo o valor 10 usado somente para representação na função mostrada na Figura 2, ou seja, o intervalo dos valores é [+7,+∞].

4.1.2. Sistema de Inferência

O sistema de inferência utiliza a função de pertinência de saída mostrada na Figura 3, onde são expressos os possíveis valores do custo *fuzzy* (*Fuzzy Cost* - FC) e seus referentes graus de pertinência. O sistema de inferência utilizou o seguinte conjunto de regras, mostrado na Tabela 1, onde são expressas as possíveis variáveis linguísticas de saídas de acordo com as variáveis linguísticas de entrada vindas do processo de fuzzificação.

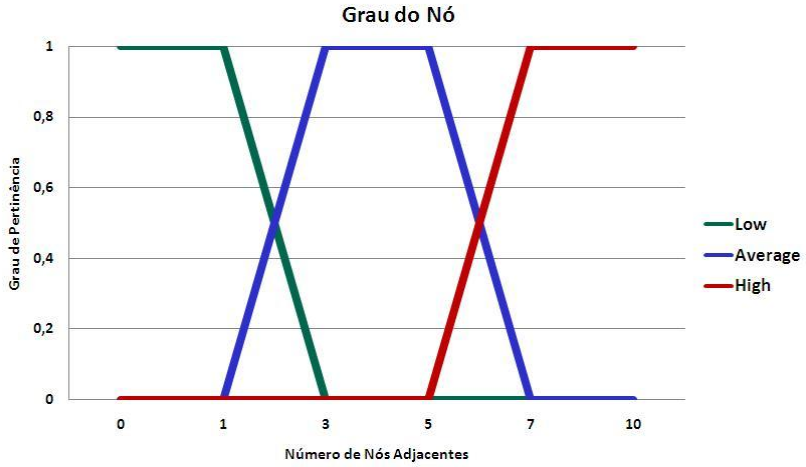


Figura 2. Função de Grau de Adjacência

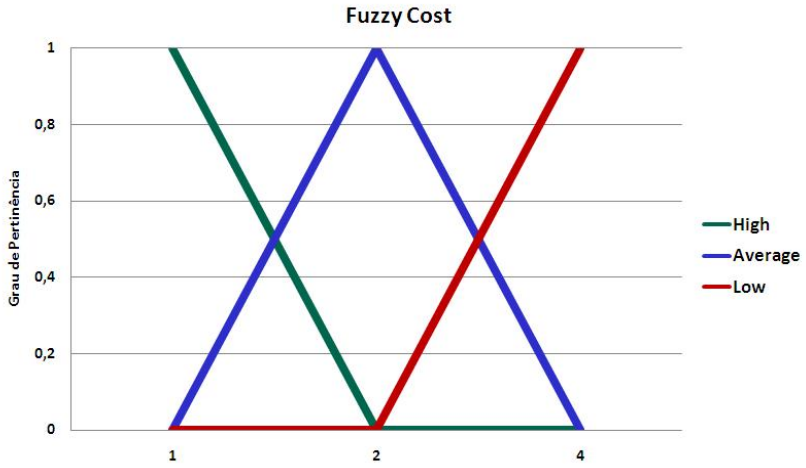


Figura 3. Função de *Fuzzy Cost*

O operador "ou", utilizado na regra 5 da Tabela 1, representa uma operação de união de dois conjuntos *fuzzy*, que pode ser representada pela função proposta por Zadeh [Zadeh 1965]: μA ∪ B = max [μA(xi), μB(xi)].

Da mesma forma o operador "e" representa a interseção entre dois conjuntos *fuzzy*, que pode ser representada pela função proposta por Zadeh [Zadeh 1965]: μA ∩ B = min [μA(xi)].

O sistema *fuzzy* proposto utilizou o modelo de inferência de Mamdani [Anderson and Hall 1999], ou seja, para todas as regras as quais o grau de pertinência, para função em questão, for maior que zero, estas irão contribuir para o cálculo de saída correspondente do sistema de inferência.

Os graus de pertinência resultantes das regras vão, por sua vez, limitar os valores dos conjuntos *fuzzy* de saída gerados por estas regras de acordo com a variável em questão, ou seja, os valores resultantes das operações feitas nas regras irão caracterizar a variável linguística resultante.

Tabela 1. Conjunto de Regras

Regra	Energia	Operação	Grau	Fuzzy Cost (FC)
1	High	e	High	High
2	High	e	Average	Average
3	Average	e	High	High
4	Average	e	Average	Average
5	Low	ou	Low	Low

A máquina de inferência tem por objetivo transformar as variáveis linguísticas de entrada em outras variáveis linguísticas correspondentes a função de pertinência de saída, no caso a função FC (Figura 3). Estas variáveis por sua vez serão convertidas em um valor *crisp*, a partir do processo de defuzzificação.

4.1.3. Defuzzificação

No processo de defuzzificação do sistema *fuzzy* proposto utilizou-se como método de defuzzificação a Média Ponderada dos Máximos [Adeli and Sarma 2006], pelo fato deste ser um método de baixo processamento e que atende o escopo da proposta. Este método produz um valor numérico considerando a média ponderada dos valores centrais ativados, sendo estes os pesos dos graus de pertinência de cada variável linguistica de saída. A função de defuzzificação pode ser visualizada na equação:

$$[(1 * \mu_H(x)) + (2 * \mu_M(x)) + (4 * \mu_L(x))]/(\mu_H(x) + \mu_M(x) + \mu_L(x))$$

Onde μ_H(x) é o grau de pertinência referente à variável *High*, μ_M(x) é o grau de pertinência referente à variável *Medium* e μ_L(x) é o grau de pertinência referente à variável *Low*. Os valores 1, 2 e 4 são os valores máximos das variáveis *High*, *Medium* e *Low*, respectivamente (Figura 3).

4.2. Princípio de Comutação em Rajadas e Fusão de Dados

A extensão proposta tem como objetivo limitar o número de pacotes enviados pela rede, para isso então implementou-se um esquema de rajadas, ou seja, periodicamente o sensor envia, caso possua dados a serem enviados, uma rajada. Essa rajada é enviada nas seguintes situações:

1. Tempo de ajuste: quando o tempo de ajuste da rajada expira esta é enviada, caso não esteja vazia. Na extensão proposta o tempo de ajuste definido foi de um segundo, ou seja, a cada um segundo a rajada é enviada;
2. Tamanho Máximo: quando a rajada atinge o tamanho máximo estipulado, esta é enviada antes do período definido, e o tempo de ajuste é reiniciado. Na extensão proposta o tamanho máximo utilizado foi de 500 bytes, ou seja, quando o tamanho total da rajada é maior do que 500 bytes esta é enviada.

O esquema descrito foi utilizado, pois como em uma rede de sensores todo o tráfego se direciona ao nó coordenador, as rajadas são sempre endereçadas ao mesmo. Sendo assim os tráfegos podem ser fundidos na rede sem problemas.

A definição de um tamanho máximo para as rajadas tem como objetivo evitar que as rajadas fiquem com tamanho excessivo, o que resultaria em uma maior probabilidade de perda destas rajadas. Sendo este um problema crítico, pois quando a rajada é perdida, perde-se os dados de vários pacotes que foram incorporados às rajadas.

5. Análise dos Resultados

Esta seção tem por objetivo apresentar o comportamento do protocolo proposto AODV-FWSN, comparado com o do protocolo AODV original. A comparação se dá a partir de simulações efetuadas no *Network Simulator* (NS-2). Na análise dos dados das simulações foi utilizado um intervalo de confiança de 99%.

O cenário utilizado para a avaliação dos protocolos foi o da rede de sensores para medição climática proposta para o campus básico da Universidade Federal do Pará (UFPA), mostrado na Figura 4. O nó 0 representa o coordenador, ou seja, todo o tráfego da rede flui para este nó.

Figura 4. Cenário Utilizado

As simulações tem por objetivo mostrar o impacto dos protocolos de roteamento no consumo de energia dos nós sensores e na perda das informações transmitidas. Os parâmetros utilizados nas simulações são mostrados na Tabela 2. Os parâmetros utilizados foram baseados nos encontrados na literatura, como nas referências [Zhu et al. 2009] e [Kalantari and Shayman 2004].

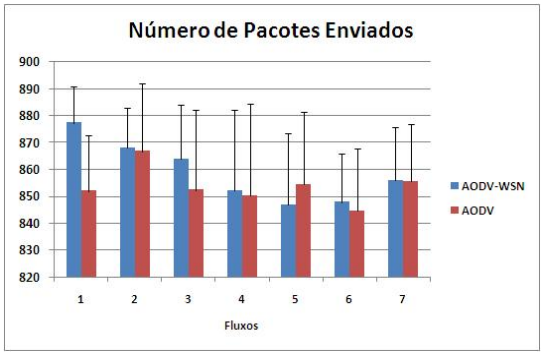
Tabela 2. Parâmetros de Simulação

Parâmetros	Valores
Energia para Transmissão	0,3 *Watts*
Energia para Recepção	0,2 *Watts*
Energia Inicial dos Nós	20 *Watts*
Energia no Modo *Sleep*	0,000000144 *Watts*
Energia no Modo *Idle*	0,00072 *Watts*
Protocolo MAC	802.15.4

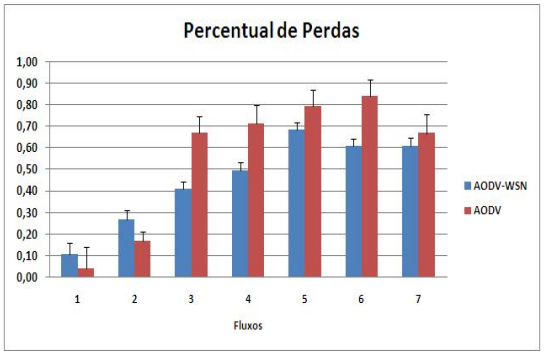
Foram gerados sete tráfegos Poisson nos sensores 1, 4, 7, 9, 14, 18 e 21 em direção ao sensor coordenador (nó 0), sendo que estes iniciaram nos tempos de 31 a 37 segundos na ordem mostrada, onde cada fluxo teve a duração de 460 segundos.

A posição dos fluxos teve como objetivo distribuir os tráfegos gerados para uma maior ocupação da rede, assim exaltando as decisões de roteamento, e o impacto destas sobre a rede.

As simulações tiveram a duração de 500 segundos, e foram efetuadas 20 simulações para cada protocolo. Os fluxos Poisson utilizados possuíram pacotes de 70 bytes de tamanho e taxa de 250 kbps.



(a) Pacotes Enviados



(b) Percentual de Perda de Pacotes

Figura 5. Gráficos de Número de Pacotes Enviados e de Percentual de Perda

A Figura 5(a) apresenta o número médio de pacotes enviados por cada protocolo em relação aos fluxos definidos. Devido ao tráfego utilizador ser Poisson, este gera pacotes simulando a geração de eventos que não ocorrem constantemente, sendo assim pode-se ter a geração de diferentes quantidades de pacotes em cada simulação.

A Figura 5(b) mostra o percentual de perda médio de cada fluxo. Nota-se que o protocolo AODV-FWSN consegue uma maior eficiência quando se trata dos tráfegos de maior distância, fluxos de 3 a 7, devido ao critério de roteamento mais eficaz, ou seja, devido ao uso do custo *fuzzy*.

Entretanto, nos fluxos 1 e 2, o protocolo AODV obtêm um desempenho superior, pois estes por serem fluxos mais próximos do coordenador acabam não necessitam de um critério eficiente para definição de rotas, visto que os nós envolvidos nestes fluxos podem alcançar o coordenador com apenas um salto, ou seja, são vizinhos diretos.

Dentro deste contexto, quando ocorrem perdas o protocolo AODV-FWSN acabam perdendo mais informações, pois este incorpora todas as informações recebidas em raja-

das, que são enviadas periodicamente, ou seja, a perda de uma rajada acaba implicando na perda de mais de uma informação.

Os dados referentes à energia de cada nó durante as simulações foram divididos em seis gráficos. São mostrados os gráficos referentes às três primeiras simulações de cada protocolo.

Este esquema foi feito, pois de acordo com as rotas determinadas em cada simulação, a energia dos nós utilizados acaba mais rápido, sendo assim a utilização da média de energia se tornaria algo inviável, que não retrataria o real consumo de energia dos nós.

Visando proporcionar uma melhor visualização do consumo de energia, os gráficos de energia em relação ao tempo de cada um dos protocolos são mostrados separadamente.

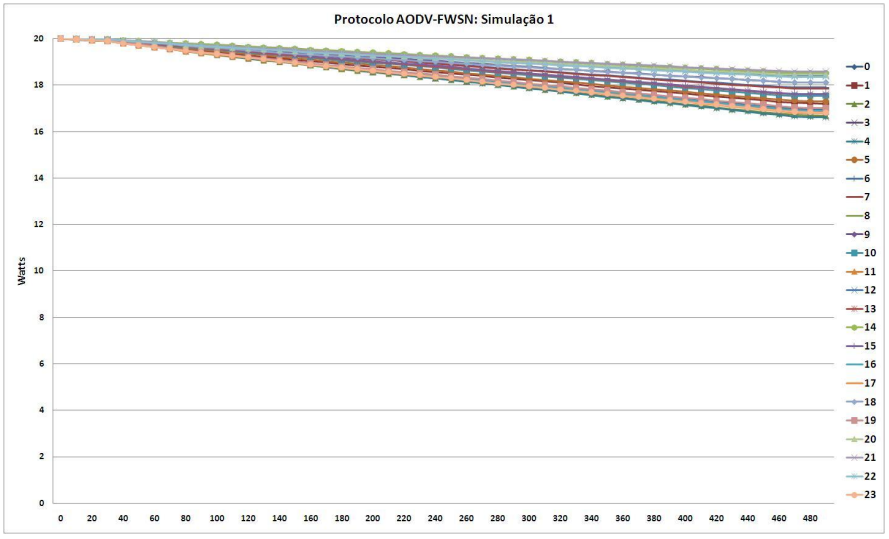


Figura 6. Simulação 1 do Protocolo AODV-FWSN

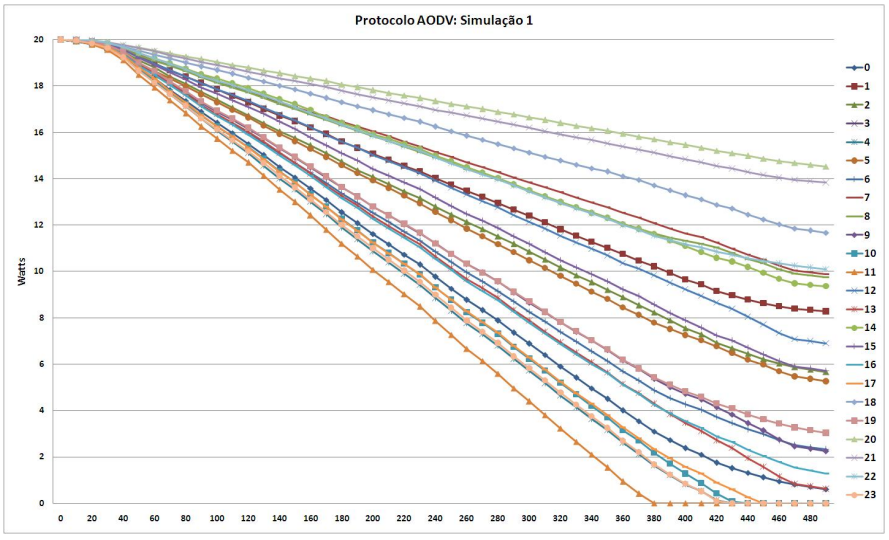


Figura 7. Simulação 1 do Protocolo AODV

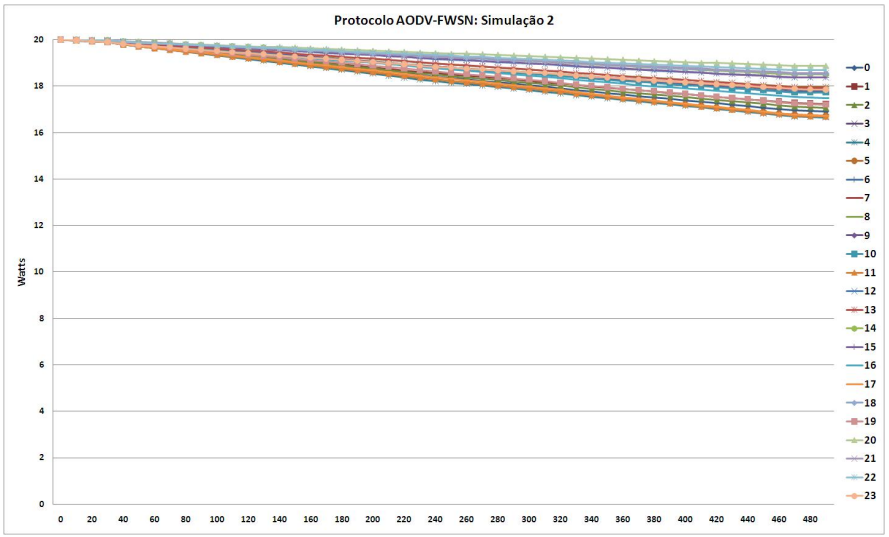


Figura 8. Simulação 2 do Protocolo AODV-FWSN

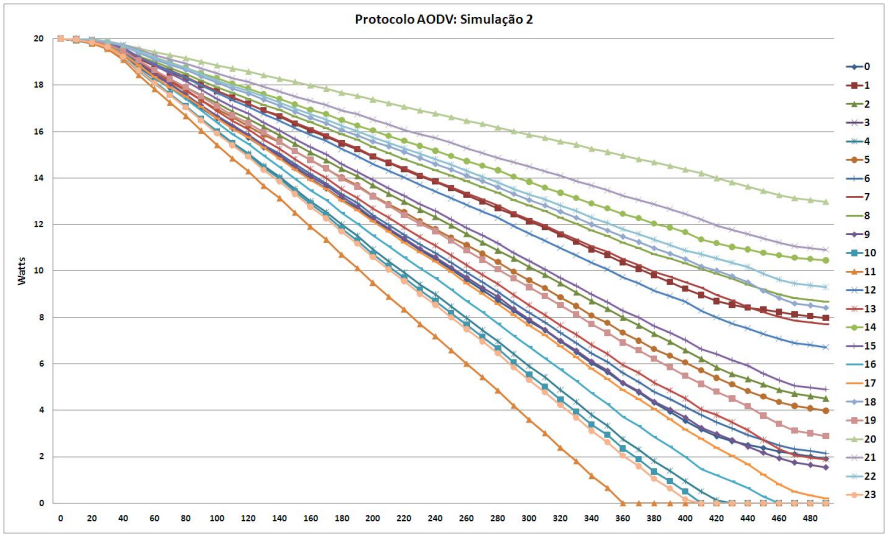


Figura 9. Simulação 2 do Protocolo AODV

As Figuras 7, 9 e 11 mostram os valores de energia dos nós em relação ao tempo de simulação quando usado o protocolo AODV. E nas Figuras 6, 8 e 10 encontram-se os valores referentes à utilização do protocolo AODV-FWSN.

A partir dos dados mostrados, percebe-se que o uso do protocolo AODV-FWSN consegue-se aumentar a vida útil da rede ao efetuar a fusão de dados que passam pelos sensores e realizar o roteamento baseado na energia restante dos nós junto com o grau de adjacência de cada um dele, isto é baseado no custo *fuzzy* que proporciona ao protocolo a capacidade de distribuir melhor os tráfegos, entre os sensores que seriam mais adequados.

Estas características tornam o protocolo mais viável em cenários onde a utilização do roteamento com vários saltos é necessária, e é algo vital para a vida útil da rede. Além de claro garantir uma eficiência na entrega das informações para o nó coordenador.

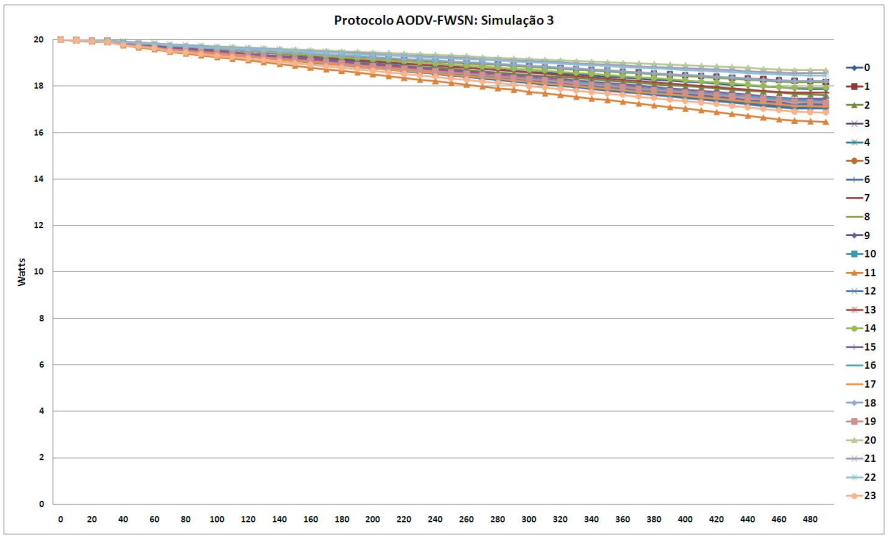


Figura 10. Simulação 3 do Protocolo AODV-FWSN

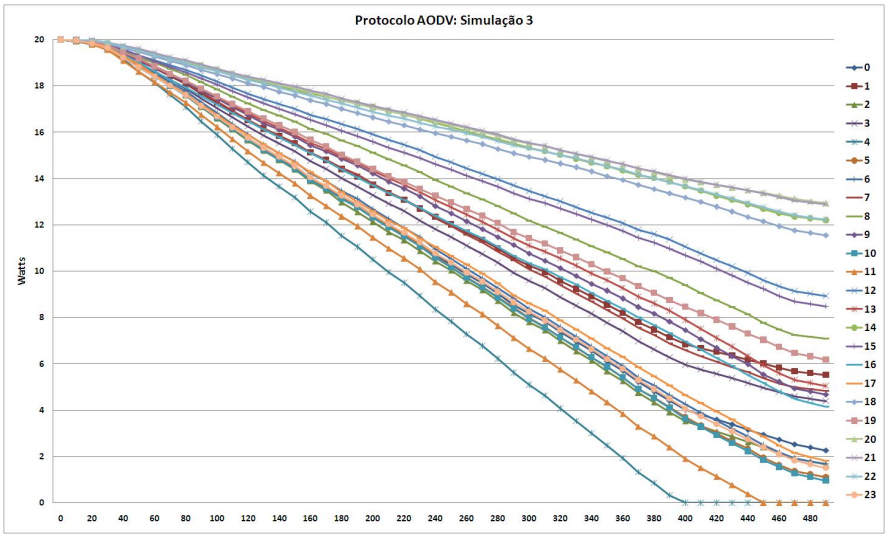


Figura 11. Simulação 3 do Protocolo AODV

6. Conclusão e Trabalhos Futuros

Este artigo apresentou uma versão para o protocolo AODV voltado para redes de sensores, o protocolo AODV-FWSN, que visa aumentar a vida útil da rede através da utilização de envio dos dados por rajadas, fusão dos dados e roteamento baseado na utilização de um custo *fuzzy*.

O custo *fuzzy* é baseado na informações de energia e grau de adjacência de um determinado nó, estas informações são usadas para se escolher rotas onde o nó em questão possua um bom nível de energia e que a chance de ocorrência da fusão de dados seja maior.

Os resultados mostraram que o AODV-FWSN consegue aumentar a vida útil da rede e manter o nível de eficiência na entrega dos pacotes, fazendo com que o protocolo AODV-FWSN consiga obter um desempenho superior ao do protocolo AODV.

Como trabalhos futuros pretende-se implementar um processo de escalonamento entra as rotas, desenvolver esquema de prioridade nas rajadas para as informações emergenciais e adequar o protocolo ao contexto de redes de sensores multimídia.

Referências

Adeli, H. and Sarma, K. C. (2006). *Cost Optimization of Structures: Fuzzy Logic, Genetic Algorithms, and Parallel Computing*. Wiley.

Akkaya, K. and Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3:325–349.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). A survey on sensor networks. *Communications Magazine, IEEE*, 40(8):102–114.

Anderson, D. and Hall, L. (1999). Mr. fis: Mamdani rule style fuzzy inference system. *IEEE International Conference on Systems, Man, and Cybernetics.*, vol.5:238–243.

Ding, W., Iyengar, S. S., Kannan, R., and Rummler, W. (2004). Energy equivalence routing in wireless sensor networks. *Microprocessors and Microsystems*, 28.

Kalantari, M. and Shayman, M. (2004). Energy efficient routing in wireless sensor networks. In *in Proc. Conference on Information Sciences and Systems, Princeton*.

Perkins, C. E., Royer, E. M., and Das, S. R. (2002). Ad hoc on-demand distance vector (aodv) routing. *IETF INTERNET DRAFT, MANET working group*.

Pinto, A. R., Benedito, B., Dantas, M., and Montez, C. (2007). Fusão de dados tempo real em redes de sensores sem fio multimídia. *XIII Simpósio Brasileiro de Sistemas Multimídia e Web (Webmedia'07), Gramado/RS*, pages 95–102.

Salustiano, R. E., , and dos Reis Filho, C. A. (2007). Sistema de fusão de sensores destinado ao monitoramento remoto de ambientes. *Simpósio Brasileiro de Sensoriamento Remoto (SBSR)*, pages 7087–7093.

Zadeh, L. (1965). Fuzzy sets. *Information and Control*.

Zhu, J., Zhao, H., and Xu, J. (2009). An energy balanced reliable routing metric in wsns. *Scientic Reasearch Publishing - Wireless Sensor Network. Disponível em: http://www.SciRP.org/journal/wsn*, pages 22–26.

Índice por Autor

A

Abelém, A. J. G. 157,185
Albuquerque, C. V. N. 59
Alencar, M. S. 43
Almeida, J. M. 3
Andreis, F. G. 103
de Araujo, R. C. A. 147
Assis, K. D. R. 87

B

Barbosa, P. E. 3
Belém, D. 131
Bianchin, L. A. 103

C

Cerqueira, E. 157
Cordeiro, W. L. da C. 103

D

Dalmazo, B. L. 103
Duarte-Figueiredo, F. 131

F

Fischer, A. J. 73
Fonseca, M. S. P. 147
Fuscaldi, F. V. B. 17

G

Gaspary, L. P. 103
Giozza, W. F. 87
Gomes, R. L. 185
Granville, L. Z. 3,103
Guimarães, L. L. 171

J

Jamhour, E. 29,73
Júnior, P. R. L. 43
Junior, W. R. P. 117

L

Loureiro, A. A. F. 117,171
Lunardi, R. C. 103

M

Monteiro, D. 185
Mota, E. S. 171
Murta, C. D. 17

N

Nascimento, V. de B. 157
Neto, A. 157
Nogueira, J. M. S. 3
Nunes, T. 185

O

Oliveira, H. A. B. F. 171
Oliveira, R. A. R. 117

P

Pinheiro, B. A. 157

R

Rodrigues, R. T. 171

S

Salvador, E. M. 3
Santos, A. F. 87
dos Santos, R. L. 103
Savasini, M. S. 87
de Sousa, A. L. R. 103
e Souza, F. R. 59

T

Taynnan, M. 43

V

Vicentini, C. J. A. 147

W

Wickboldt, J. A. 103
Wowk, R. M. S. 29