



**UNIVERSIDADE FEDERAL DE SANTA CATARINA – UFSC**  
**DEPARTAMENTO DE INFORMÁTICA E DE ESTATÍSTICA – INE**  
**CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO - CPGCC**  
**LABORATÓRIO DE REDES E GERÊNCIA - LRG**

# **Projeto TAGERE**

## **Tópicos Avançados em Gerência de Redes de Computadores e Telecomunicações**

**Projeto Integrado de Pesquisa - AI**

<b>1. TÍTULO</b>	<b>4</b>
<b>2. INTRODUÇÃO</b>	<b>4</b>
2.1 ANTECEDENTES.....	4
2.2 ESTADO-DA-ARTE.....	6
2.3 MOTIVAÇÃO.....	6
2.4 CARACTERIZAÇÃO DO PROBLEMA.....	6
2.5 JUSTIFICATIVAS.....	6
<b>3. OBJETIVOS E RESULTADOS ESPERADOS</b>	<b>6</b>
3.1 OBJETIVOS.....	6
3.2 RESULTADOS ESPERADOS.....	7
3.3 APROVEITAMENTO DOS RESULTADOS.....	7
<b>4. METODOLOGIA</b>	<b>7</b>
<b>5. EQUIPE EXECUTORA</b>	<b>10</b>
5.1 MEMBROS DA EQUIPE EXECUTORA.....	10
<b>6. CRONOGRAMA FÍSICO E DE EXECUÇÃO</b>	<b>11</b>
<b>7. DESCRIÇÃO MAIS DETALHADA DAS ATIVIDADES DE PESQUISA</b>	<b>14</b>
7.1 Refinamento e Validação de Políticas de Segurança e Segurança Multilateral.....	14
7.2 Framework RBAC (Role Based Access Control) para Aplicações Web.....	16
7.3 Autenticação fim-a-fim para o LDP (Label Distribution Protocol) na Arquitetura MPLS.....	19
7.4 IDS e Compartilhamento e Atualização de Bases de Assinaturas Utilizando Agentes Móveis.....	21
7.5 Aplicação de Inteligência Computacional (Lógica <i>Fuzzy</i> e Redes Neurais) na Gerência de Redes através da Automatização do uso de Agentes Móveis.....	23
7.6 Arquitetura de <i>Grids</i> de Agentes Aplicada à Gerência de Redes.....	25

7.7 Gerência de Redes em Ambientes WEB, WAP e SMS usando as Tecnologias SNMP, WBEM e CORBA.....	27
7.8 Gerência de Acordos de Níveis de Serviços para Redes Sem Fio.....	29
7.9 Qualidade de Serviço (Perdas de pacotes, Latência e <i>Jitter</i> ) em Redes Sem Fio Ad Hoc.....	32
7.10 Reconhecimento de Padrões através de Redes Bayesianas e Algoritmo Genético Aplicado à Gerência de Segurança.....	34
7.11 Aplicações de XML para Auxiliar na Gerência de Redes.....	36
7.12 Gerenciamento de Serviços baseados em Políticas sobre Redes de Serviços Diferenciados.....	38
7.13 Licenças para Distribuição de Conteúdo Online em Sistemas DRM Usando a Linguagem XrML.....	39
<b>8. CONTRAPARTIDA</b>	<b>41</b>
<b>9. ORÇAMENTO</b>	<b>41</b>
<b>10. AGRADECIMENTOS</b>	<b>43</b>
<b>11. REFERÊNCIAS BIBLIOGRÁFICAS</b>	<b>43</b>

## 1. **TÍTULO**

Projeto TAGERE – Tópicos Avançados em Gerência de Redes de Computadores e Telecomunicações.

## 2. **INTRODUÇÃO**

### 2.1 **Antecedentes**

Os componentes do Grupo de Redes e Gerência da UFSC têm boa experiência na área de redes e gerência deste ambiente, atuando em:

- 1) no desenvolvimento do sistema de gerência do projeto ESPRIT 2100 - MAX (Metropolitan Area Communication System) da CEE (Comunidade Econômica Européia), onde o Coordenador Geral deste projeto Integrado de Pesquisa submetido ao CNPq foi líder do Projeto MAX junto à Université Paul Sabatier (Toulouse-France) representando a mesma na CEE (atual UE).
- 2) no desenvolvimento de projetos de gerência de redes na UFSC e na UFRGS desde 1985;
- 3) na organização de eventos científicos nacionais e internacionais em redes e gerência de redes desde 1983;
- 4) Projeto integrado de Pesquisa submetido ao CNPq em 18/02/94.  
Título: Projeto de uma plataforma aberta para gerência de redes.  
Objetivo: Realização de estudos e desenvolvimentos sobre plataformas e sistemas de gerenciamento, buscando a integração do gerenciamento de sistemas em ambientes heterogêneos.
- 5) Projeto CNPq/ProTeM-CC-II/PLAGERE submetido em 04/04/94.  
Título: PLAGERE - Plataformas para Gerência de Redes  
Objetivo: Realização de estudos comparativos e novos desenvolvimentos em plataformas padronizadas e proprietárias; Concepção de uma plataforma genérica com o uso de formalismos algébricos; Desenvolvimentos para gerência de redes de alta velocidade; e Estudos de conformidade e interoperabilidade de redes heterogêneas.
- 6) Projeto Integrado de Pesquisa submetido ao CNPq em 26/02/97.  
Título: AUTOGERE – Automação e Distribuição da Gerência de Redes.  
Objetivos: Estudos, comparações e desenvolvimento de aplicações para gerência de redes de alta velocidade; Estudos, análises e desenvolvimento de aplicações para a automatização da gerência (gerência proativa); e Estudos, análise e desenvolvimento para a conformidade e a interoperabilidade da gerência de redes;
- 7) Sub-Projeto Intitulado Gerenciamento de Recursos ATM do Projeto RMAV-FLN (Rede Metropolitana de Alta Velocidade de Florianópolis) fomentado por RNP/PROTEM-CC a partir de outubro de 1998.
- 8) Projeto Integrado de Pesquisa submetido ao CNPq em 28/02/99  
Título: GERDIM – Gerência em Redes Distribuídas e Móveis.  
Objetivos: Estudos e proposições sobre o uso de probabilidade e estatística na gerência de redes; Continuidade dos estudos e proposições sobre o emprego de inteligência artificial (sistemas especialistas e redes neurais) na gerência de redes; e Análise e emprego de políticas, mecanismos e serviços de segurança na gerência de redes; e realização e avaliação da gerência de redes através de plataformas distribuídas.
- 9) Projeto Integrado de Pesquisa submetido ao CNPq em 02/03/2001  
Título: HOPE – “Hot Topics” em Gerência de Redes  
Objetivos: Desenvolvimento de novas aplicações para gerência de redes de alta velocidade; Desenvolvimento de novas aplicações para a automatização da gerência (gerência proativa); Continuidade dos estudos, análise e desenvolvimento da gerência de redes sem fio; Continuidade dos estudos e proposições sobre o uso de probabilidade e estatística na gerência de redes; Continuidade dos estudos e proposições sobre o emprego de inteligência artificial (sistemas especialistas e redes neurais) na gerência de redes; Continuidade da análise e emprego de políticas, mecanismos e serviços de segurança na gerência de redes; Continuidade da avaliação de plataformas e agentes móveis na gerência de redes; Estabelecer os requisitos necessários correspondentes a cada tema de pesquisa; Desenvolvimento de novas aplicações de gerência distribuída nos temas de pesquisa abordados neste projeto; e Contribuir para o avanço teórico, experimental e prático dos temas de pesquisa apresentados acima.

## Relação de Projetos

### Anteriores

- **desenvolvimento do sistema de gerência do projeto ESPRIT 2100 - MAX** (*Metropolitan Area Communication System*) da CEE (Comunidade Econômica Européia), onde o líder deste projeto submetido ao ProTeM-CC foi líder do Projeto MAX junto à *Université Paul Sabatier* (Toulouse-France) representando a mesma na CEE.
- desenvolvimento de projetos de gerência de redes na UFSC e na UFRGS;
- **Projeto integrado de Pesquisa submetido ao CNPq em 18/02/94.**  
**Título:** Projeto de uma plataforma aberta para gerência de redes.  
**Objetivos:** Realização de estudos e desenvolvimentos sobre plataformas e sistemas de gerenciamento, buscando a integração do gerenciamento de sistemas em ambientes heterogêneos.
- **Projeto CNPq/ProTeM-CC-II/PLAGERE submetido em 04/04/94.**  
**Título:** PLAGERE - Plataformas para Gerência de Redes  
**Objetivos:** Realização de estudos comparativos e novos desenvolvimentos em plataformas padronizadas e proprietárias; Concepção de uma plataforma genérica com o uso de formalismos algébricos; Desenvolvimentos para gerência de redes de alta velocidade; e Estudos de conformidade e interoperabilidade de redes heterogêneas.
- **Projeto Integrado de Pesquisa AUTOGERE submetido ao CNPq em 26/01/97.** **Título:** AUTOGERE – Automação da Distribuição da Gerência de Redes. **Objetivos:** Entre os objetivos do Projeto AUTOGERE destacam-se: Estudos, análises e comparações das dificuldades e soluções encontradas no gerenciamento de Redes de Telecomunicações e Redes de Computadores; Estudos, comparações e desenvolvimento de aplicações para gerência de redes de alta velocidade; Estudos, análises e desenvolvimento de aplicações para a automatização da gerência (gerência proativa); Estudos, análise e desenvolvimento para a conformidade e a interoperabilidade da gerência de redes; Dar tratamento formal ao desenvolvimento e à validação de sistemas para gerência de redes; e Estudos sobre as posições atuais e perspectivas dos organismos de padronização.
- **Projeto RMAV-FLN** (Rede Metropolitana de Alta Velocidade na Região de Florianópolis), suportado pelo CNPq-PROTEM/RNP. **Objetivos:** promover a implantação das tecnologias adequadas à nova geração de serviços e aplicações da Internet, ainda que em ambientes limitados; capacitar pessoal técnico de universidades e centros de pesquisa para operar e utilizar a nova geração de ferramentas e aplicações da Internet; contribuir para estabelecer as condições necessárias para administração e operação de um backbone nacional de alta velocidade.
- **Projeto Integrado de Pesquisa submetido ao CNPq em 28/02/99.**  
**Título:** GERDIM – Gerência em Redes Distribuídas e Móveis.  
**Objetivos:** Estudos e proposições sobre o uso de probabilidade e estatística na gerência de redes; Continuidade dos estudos e proposições sobre o emprego de inteligência artificial (sistemas especialistas e redes neurais) na gerência de redes; Análise e emprego de políticas, mecanismos e serviços de segurança na gerência de redes; e realização e avaliação da gerência de redes através de plataformas distribuídas.

### Atual

**Projeto Integrado de Pesquisa HOPE submetido ao CNPq em 02/03/2001.** **Título:** HOPE – “Hot Topics” em Gerência de Redes.

**Objetivo:** Desenvolvimento de novas aplicações para gerência de redes de alta velocidade; Desenvolvimento de novas aplicações para a automatização da gerência (gerência proativa); Continuidade dos estudos, análise e desenvolvimento da gerência de redes sem fio; Continuidade dos estudos e proposições sobre o uso de probabilidade e estatística na gerência de redes; Continuidade dos estudos e proposições sobre o emprego de inteligência artificial (sistemas especialistas e redes neurais) na gerência de redes; Continuidade da análise e emprego de políticas, mecanismos e serviços de segurança na gerência de redes; Continuidade da avaliação de plataformas e agentes móveis na gerência de redes; Estabelecer os requisitos necessários correspondentes a cada tema de pesquisa; Desenvolvimento de novas aplicações de gerência distribuída nos temas de pesquisa abordados neste projeto; e Contribuir para o avanço teórico, experimental e prático dos temas de pesquisa apresentados acima.

## 2.2 Estado-da-arte

Os principais problemas associados à implementação e uso da gerência de redes ocorrem devido à grande quantidade de padrões e de diferentes produtos oferecidos no mercado, dificultando consideravelmente a tomada de decisão no que se refere a utilização da plataforma de gerência mais adequada. Além disso, novas tendências na área de gerência de redes vêm sendo pesquisadas, entre estas destacam-se, a gerência proativa, distribuição da gerência de redes, gerência para redes distribuídas, gerência de redes móveis e sem fio, gerência em segurança de redes, uso de inteligência artificial em gerência de redes e uso da tecnologia Web na gerência de redes. Além do emprego de gerência de redes baseada em políticas, políticas de segurança, segurança multilateral, agentes móveis, redes neurais, redes bayseanas, algoritmos genéticos, lógica fuzzy, multi-agentes e *grids* de agentes. Estas novas tendências vêm sendo pesquisadas no Laboratório de Redes e Gerência (LRG) da UFSC e a partir deste projeto as mesmas poderão ser aperfeiçoadas.

## 2.3 Motivação

Devido à explosão de complexidade dos serviços exigidos e do tamanho das redes de computadores e telecomunicações, novos conceitos devem ser agregados ao gerenciamento dessas redes. A urgência do desenvolvimento, emprego e aperfeiçoamento dos seguintes conceitos é muito importante:

- Gerência de redes através de *grids* de agentes e multi-agentes;
- Gerência automatizada (proativa);
- Gerência em redes sem fio;
- Gerência de segurança através de políticas;
- Gerência com Inteligência artificial distribuída;
- Gerência com tecnologia Web, WAP, WBEM e CORBA;
- Gerência com agentes móveis;
- Distribuição da gerência de redes;
- Gerência usando lógica fuzzy e redes neurais;
- Gerência usando redes bayseanas e algoritmos genéticos; e
- Gerência de QoS através de políticas.

## 2.4 Caracterização do problema

Na seção 7 (Descrição mais detalhada das atividades de pesquisa) os problemas associados aos tópicos apresentados acima são caracterizados.

## 2.5 Justificativas

Na seção 7 (Descrição mais detalhada das atividades de pesquisa) as justificativas associados aos tópicos apresentados acima são apresentadas.

# 3. OBJETIVOS E RESULTADOS ESPERADOS

## 3.1 Objetivos

Entre os objetivos do Projeto TAGERE destacam-se:

- 1) Desenvolvimento de novos resultados para gerência de redes baseada em políticas;
- 2) Desenvolvimento de novas aplicações para a automatização da gerência (gerência proativa);

- 3) Continuidade dos estudos, análise e desenvolvimento da gerência de redes sem fio;
- 4) Continuidade dos estudos e proposições sobre o uso de probabilidade e estatística na gerência de redes;
- 5) Continuidade dos estudos e proposições sobre o emprego de inteligência artificial (sistemas especialistas, redes neurais, redes bayesianas, algoritmos genéticos e lógica fuzzy) na gerência de redes;
- 6) Continuidade da análise, aperfeiçoamento e emprego de políticas, mecanismos e serviços de segurança na gerência de redes;
- 7) Continuidade dos aperfeiçoamentos sobre gerência de redes através de agentes móveis, multi-agentes e grids de agentes;
- 8) Estabelecer os requisitos necessários e apresentar soluções para cada tema de pesquisa mencionado acima;
- 9) Aperfeiçoamento e desenvolvimento de novas aplicações de gerência distribuída nos temas de pesquisa abordados neste projeto;
- 10) Contribuir para o avanço teórico, experimental e prático dos temas de pesquisa apresentados acima.

Na seção 7 (Descrição mais detalhada das atividades de pesquisa) são apresentados mais objetivos associados a cada atividade que será desenvolvida no projeto TAGERE.

### **3.2 Resultados esperados**

A seguir são apresentados alguns resultados esperados, considerando a realização dos objetivos anteriormente apresentados.

- 1) Relatórios de pesquisa propondo novas funções para o gerenciamento de redes baseado em políticas. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementação das novas funções propostas.
- 2) Relatório de pesquisa propondo soluções para automatização do gerenciamento de redes. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementação de um protótipo.
- 3) Relatórios de pesquisa propondo soluções para gerenciamento em segurança de redes. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementação das políticas, mecanismos e serviços de segurança.
- 4) Relatórios de pesquisa propondo soluções e relatando experiências sobre o uso da tecnologia Web, WBEM, WAP e CORBA na gerência de redes. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementações de protótipos.
- 5) Relatórios de pesquisa apresentando experiência do emprego de redes neurais, sistemas especialistas, algoritmos genéticos, lógica fuzzy e métodos estatísticos na gerência de redes. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementações de protótipos.
- 6) Relatórios de pesquisa propondo soluções para uma nova arquitetura de redes através da tecnologia de agentes móveis, multi-agentes, grids de agentes e redes sem fio, aplicado também à gerência de redes de telecomunicações. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementação de um protótipo.
- 7) Relatórios de pesquisa propondo soluções para a definição de novos serviços programáveis pelo usuário, sobre elementos de redes. Relatórios de atividade relatando o desenvolvimento desta tarefa. Implementação de um protótipo.

Na seção 7 (Descrição mais detalhada das atividades de pesquisa) são apresentados mais resultados esperados em cada atividade que será desenvolvida no projeto TAGERE.

### **3.3 Aproveitamento dos resultados**

Os resultados podem ser aproveitados por diversas organizações públicas e privadas, auxiliando no desenvolvimento, na aquisição, aperfeiçoamento e no uso de um sistema de gerenciamento que contemple o estado-da-arte atual. Além disso, as instituições de pesquisa e empresas também poderão aproveitar os resultados diretamente nas suas redes, proporcionando crescimento destes grupos de pesquisa tanto em quantidade como em qualidade. Estes resultados deverão ser submetidos a publicação em periódicos e anais de conferências nacionais e internacionais. Ainda como resultado deve ser evidenciada a contribuição para formação de recursos humanos a nível de graduação e pós-graduação (mestrado e doutorado), além de contribuir para o desenvolvimento científico e tecnológico do país.

## **4. METODOLOGIA E ESTRATÉGIA DE AÇÃO**

A metodologia e a estratégia de ação para o desenvolvimento do Projeto TAGERE está baseada na execução de atividades. Cada pesquisador estará associado a uma ou mais atividade, e deverá ser auxiliado pelos colaboradores e estudantes (graduação e pós-graduação). Cada atividade é indicada por uma letra. O período de realização de uma atividade pode ser facilmente observado nos cronogramas apresentados. Os períodos de revisão de uma atividade são realizados a cada três meses. Cada atividade é coordenada por um pesquisador, com a cooperação de colegas com pós-doutorado, doutorado, doutorandos, mestrandos e graduandos dos Cursos de Graduação e Pós-Graduação em Ciência da Computação. Em relação ao

desenvolvimento técnico e científico serão empregados os mesmos métodos utilizados nos projetos anteriores de gerência de redes, onde os resultados são alcançados, considerando as experiências anteriores e técnicas usadas pelas melhores instituições internacionais de pesquisa na área (inclusive baseando-se nos próprios resultados de pesquisa anteriormente obtidos pela nossa equipe). A partir destes trabalhos o Grupo de Redes e Gerência da UFSC identifica pendências e propõe soluções.

### Descrição sucinta das atividades

- Atividade A Nesta atividade serão aperfeiçoados os estudos, análises e desenvolvimento de métodos para a gerência de segurança distribuída. Esta atividade apresenta um trabalho original e inédito, com o refinamento ou a reescrita das propriedades fundamentais do modelo de segurança *Chinese Wall* [Brewer e Nash 1989], considerando o conceito de segurança multilateral, com o objetivo de facilitar o seu entendimento e sua implementação. A atividade também implementa a política de segurança *Chinese Wall* considerando um ambiente comercial de consultoria de empresas.
- Atividade B Nesta atividade serão continuados e aperfeiçoados a criação de um *framework* baseado no modelo de segurança RBAC e que possa ser utilizado por aplicações Web. Este *framework* é composto por várias classes (concretas e abstratas) que implementam mecanismos de autenticação, controle de acesso, auditoria e administração. A utilidade deste *framework* está na diminuição do tempo de desenvolvimento da parte de segurança de aplicações Web ou de aplicações Java que utilizem a política de papéis.
- Atividade C Nesta atividade serão aperfeiçoados os estudos e desenvolvimentos associados a uma solução de autenticação fim a fim para o protocolo LDP, de modo a preencher esta lacuna do protocolo, viabilizando o estabelecimento de LSPs entre dois LSRs não-adjacentes. A solução de autenticação fim-a-fim, foi planejada para ambientes onde LSPs atravessam múltiplos domínios externos, considerados não confiáveis, e que por isso necessitam se autenticar durante o estabelecimento de um novo LSP. *Conforme foi verificado pelo levantamento de trabalhos correlatos [DE CLERCQ, 2001], [BUDA, 2001], [KENT, 2000], [BADAN, 2001], atualmente é desconhecida uma solução de autenticação semelhante, que efetivamente atenda o propósito de autenticar num escopo fim-a-fim, o estabelecimento de LSPs dentro do protocolo LDP. Dessa forma a solução proposta por este trabalho é inédita dentro do seu escopo de aplicação.*
- Atividade D Nesta atividade serão aperfeiçoados os trabalhos associados a uma arquitetura que proporcione a atualização automática da base de assinaturas de um IDS. Esta atualização será feita através de agentes móveis que realizam consultas em bases de assinaturas de outros IDSs, espalhadas pela Internet. Como objetivos específicos temos: desenvolvimento de uma estrutura para o armazenamento das assinaturas; desenvolvimento de uma estrutura para publicação da base de assinaturas, de forma a possibilitar a consulta destas assinaturas; e desenvolvimento de agentes móveis capazes de consultar e copiar assinaturas de bases publicadas por IDSs.
- Atividade E Esta atividade visa aperfeiçoar os desenvolvimentos implementados sobre um *framework* de agentes móveis, o KDEMA (desenvolvido pela equipe). Podemos utilizar inteligência computacional no apoio a decisão. Pesquisas que utilizam inteligência computacional em agentes móveis também podem ser encontrados, como em [Karnouskos 2002], onde uma combinação neuro-fuzzy é utilizada para propor um sistema de mensagens inteligente e dinâmico, adaptável às condições do usuário. Em [Das 2002] temos inteligência computacional atuando na distribuição de tarefas a agentes móveis para resolução de pesquisas complexas em bases distribuídas. As métricas analisadas foram tempo e tamanho das pesquisas. Ele apresenta três configurações de pesquisa: um agente, múltiplos agentes ou pesquisa convencional, e sem agentes.
- Atividade F Nesta atividade serão aperfeiçoados os desenvolvimentos anteriores considerando que no fluxo de trabalho tradicional do gerenciamento de redes temos uma situação onde dados são extraídos dos equipamentos e precisam ser transformados em informações que possam orientar o gerente na tomada de decisões e na execução de ações de gerenciamento [Koch e Westphall 2001]. Sistemas baseados em regras de produção e inferência podem ser utilizados para analisar estes dados, extrair as informações necessárias e identificar possíveis problemas. Porém, a consolidação destes dados em informações de gerência é

uma tarefa intensiva e consome um grande poder de processamento. À medida que o ambiente cresce, a eficiência de um sistema centralizado diminui e aumenta o custo com hardware. Esta atividade apresenta uma arquitetura alternativa, baseada em *grids* de agentes para distribuir a carga destas tarefas intensivas do gerenciamento.

- Atividade G Nesta atividade serão evidenciados o uso das características de implementações baseadas na iniciativa WBEM, juntamente com os já consagrados SNMP e CORBA, através de uma aplicação baseada nos conceitos de engenharia de software foi possível criar uma aplicação completa para gerenciar uma rede, flexível para criação de aplicativos com diversos enfoques. Com a interface dessa aplicação sendo feita baseada na WEB, é possível gerenciar uma rede a partir de qualquer lugar do mundo onde se tenha uma conexão à Internet. As vantagens de usar esse tipo de interface são várias, indo desde a substituição da linha de comando até a economia em treinamento de pessoas especializadas [MAC01]. Além disso, para proporcionar um melhor acesso a informações gerenciais, a utilização de dispositivos WAP vem crescendo ao longo dos últimos anos devido à demanda existente [STU02]. Este protocolo, mesmo com as dificuldades existentes no ambiente *wireless*, mostra-se bastante útil se bem utilizado, principalmente como forma de apoio a ferramentas de gerência.
- Atividade H Nesta atividade serão aperfeiçoados os desenvolvimentos realizados no contexto das redes sem fio. A gerência de níveis de serviços é definida através de contratos - SLAs estabelecidos durante a fase de contratação do serviço, que é utilizado tanto pelo cliente quanto pelo provedor, para verificar os níveis de serviços providos. As tecnologias baseadas em radio frequência, surgem com bastante força no mercado, como é o caso das redes *ad-hoc*, as quais combinam funcionalidade, flexibilidade, conectividade de dados, mobilidade de usuários em diversos ambientes. Sendo assim, este trabalho tem como objetivo obter através de simulações e medições informações de desempenho nas redes sem fio *ad-hoc* e analisar estas informações a fim de moldar parâmetros de qualidade de serviço, que compõem os SLAs, providos sobre estas redes, garantindo assim o seu melhor funcionamento.
- Atividade I Aperfeiçoar os objetivos e metas deste trabalho que são realizar uma comparação entre os esquemas de filas *First In First Out (DropTail)*, em comparação com os esquemas *Fair Queueing*, *Stochastic Fair Queueing* e *Deficit Round Robin*, através da simulação de um canal ACL simétrico com 433 Kbits/seg e sentido unidirecional. Para a simulação foi utilizado o software *Network Simulator 2* [Fall e Varandhan 2001] com o objetivo de obter uma visão ampliada do comportamento dos esquemas de filas; avaliar o enfileiramento na *scatternet* e *piconet*; e avaliar a latência e o *jitter* na *scatternet*. Os resultados apresentados neste artigo são baseados nas simulações de uma *scatternet*, com um *slave* atuando como *gateway*, tráfego unidirecional. Foram tabulados os resultados da *piconet* de origem e o comportamento no *master*. Quando o tráfego está no dispositivo *master* já pode ser considerado como tráfego da *scatternet*, por destiná-lo ao nó *gateway*.
- Atividade J Aperfeiçoar os resultados associados ao problema de desenvolver um sistema probabilístico Bayesiano, com o uso do software Netica, capaz de classificar grupos de usuários da telefonia móvel celular, de acordo com suas características de utilização do serviço. De acordo com a classificação feita, os usuários pertencerão a grupos que apontam sua forma de utilizar o serviço oferecido. O que pode auxiliar a projetos que pretendem a detecção de fraude, ao serem observados comportamentos que fujam as características habituais de uso dos clientes. Algoritmo genético (AG) é uma excelente técnica tanto para resolver problemas de busca em um espaço de características, como para encontrar soluções ótimas. Inspirando-se nestas importantes características dos AGs, é desenvolvido neste trabalho um algoritmo de agrupamento baseado em algoritmo genético, utilizado na busca dos valores dos centros dos grupos.
- Atividade L Aperfeiçoar na gerência de redes, o emprego de XML para definir modelos de informação de gerenciamento e processar informação nas aplicações de gerência vem se tornando atrativo [Lewis 01]. Nesse aspecto, XML e suas tecnologias correlatas apresentam vantagens como [Martin-Flatin 00]: melhor integração dos dados gerenciados; ligação mais flexível entre o objeto gerenciado e aplicação gerente; interoperabilidade entre aplicações de gerenciamento de diferentes fabricantes; apresentação das informações gerenciais facilidade e estendida para uma ampla variedade de formatos; possibilidade de transformação automática das

informações de gerenciamento originais, agregando valor decisório nas novas informações produzidas; e validação dos dados de gerenciamento automática e centralizada.

Atividade M Nesta linha de pesquisa podemos citar os trabalhos de definição de uma linguagem para a especificação da sintaxe e semântica de políticas de serviços de rede. Onde o gerenciamento baseado em políticas poder orientar o comportamento de uma rede ou sistema distribuído, completando altos níveis declarativos e redefinindo níveis baixos para otimização geral dos recursos. Contudo a QoS é um tema de grande relevância e de real aplicabilidade para a comunidade, sendo os resultados de maior importância apresentados em diversos eventos e periódicos da área. A proposta deste trabalho se concentrara no mecanismo de serviços diferenciados, verificando suas principais características em determinadas políticas de gerenciamento de rede e analisando seus resultados.

Atividade N Gerenciamento de Direitos Digitais, pode ser encarado como um termo chave para novos processos de negócios confiáveis, uma tecnologia fundamental para proteger o comércio, a propriedade intelectual, o próprio conteúdo digital, e implementar questões relativas à privacidade. Uma definição de DRM, segundo [Maclachlan 2001]: “DRM é a corrente de software, serviços e tecnologias que limitam o uso de conteúdo digital ao uso e usuários autorizados e gerenciam quaisquer consequências deste uso durante todo o ciclo de vida do conteúdo.” Em um ambiente empresarial, DRM pode auxiliar no gerenciamento de políticas, as quais controlam o acesso e gerenciamento de informação dentro de uma organização, por exemplo [Duhl and Kevorkian 2001].

## 5. **EQUIPE EXECUTORA**

O grupo executor das tarefas no Projeto TAGERE será composto pelos professores, pesquisadores, doutorandos, mestrands e graduandos apresentados abaixo:

### 5.1 **Membros da equipe executora**

1) Professor coordenador do projeto:

- Carlos Becker Westphall (Dr. - UFSC);

2) Professores pesquisadores e colaboradores:

- Luiz Carlos Zancanella (Dr. - UFSC);
- Silvia Modesto Nassar (Dra. – UFSC);
- Ricardo Felipe Custódio (Dr. – UFSC);
- Mario Dantas (Dr. –UFSC);
- Carla Merkle Westphall (Dra. - UFSC);
- Arthur Ronald de Vallarius Buchsbaum (Dr. - UFSC);
- Fernando Augusto da Silva Cruz (Dr. - UFSC);
- Luiz Nacamura Junior (Dr. - CEFET-PR);
- Michele Sibilla (Dra. – França);
- Keith von Mecklenburg (Dr. - Escócia);
- Abderrahim Sekkaki (Dr. - Marrocos);
- Júlio Cesar da Costa Ribas (M. Sc. – CEFET-SC).

3) Pesquisadores colaboradores:

- Luis Marco Caceres Alvarez (Doutorando – UFSC);
- Alexandre Veloso Matos (Doutorando – UFSC);
- André Melo Barotto (Doutorando – UFSC);
- Abiel Roche Lima (Doutorando - UFSC);
- Fernando Luiz Koch (Doutorando - Holanda);
- André Barros (Doutorando – França);
- Elvis Vieira (Doutorando – Canada);
- Juliana Amaral Arantes (Mestre – UFSC);
- Edison Tadeu Melo (Mestre - UFSC);
- Kátyra Kowalski Armanini (Mestre – Thermus);
- Ângela Melo Barotto (Mestre – UFSC);
- Ana Lúcia Anacleto Reis (Mestre – FURB);
- Guilherme Eliseu Rhoden (Mestre – UFSC);
- Fabio Spanhol (Mestre – UNIOESTE);

- Gilson Norberto Horstmann (Mestre – Embraco);
- Douglas Nazareno Debiazi Vargas (Mestre – UNIPLAC);
- Edison Alessandro Xavier (Mestre - UFSC);
- Richard R. Reinert (Mestre – UFSC);
- Morvan Daniel Muller (Mestre – Softplan);
- Gerson Valdir dos Santos (Mestre – UFSC);
- Tom Spindola (Mestre – UFSC);
- Daniel Bitencourt Cadorin (Mestre – Unisul);
- Edivane Bellé (Mestre - UFSC);
- Rafael Plentz (Mestre - UFSC );
- Luciana Pietroski (Mestre - UFSC );
- Marcos Assunção Dias (Mestrando – UFSC);
- Madalena Pereira da Silva (Mestrando – UFSC);
- Cezar Bettoni (Mestrando – UFSC);
- Mateus Casanova Pereira (Mestrando – UFSC);
- Eduardo Bueno (Mestrando – UFSC);
- Breno Syperrek (Mestrando – UFSC);
- Paulo Fernando da Silva (Mestrando – UFSC);
- Aujor Tadeu Cavalca Andrade (Mestrando – UFSC);
- Rodrigo Santana (Mestrando – UFSC);
- Joao Carlos Redin (Mestrando – UFSC);
- Cleber V. Filippin (Mestrando – UFSC);
- Valério Rosset (Mestrando – UFSC);
- Jean Pierre Ezequiel (Mestrando – UFSC);
- Ferananda Emanuella Sillveira (Graduada - Thermus);
- Michel Lobato (Graduando – UFSC);
- Rafael Tavares (Graduando – UFSC);
- Sílvia C. C. Bianchini(Graduada – UFSC);
- Alexandre Parra (Graduando – UFSC);
- Marcel Castilho (Graduando – UFSC);
- Júlio Alexandre de Albuquerque Reis (Graduando – UFSC);
- Leonardo N. Bernardo (Graduando – UFSC);
- Eduardo Erle Santos (Graduando – UFSC);
- Daniel Quadros da Silva (Graduando – UFSC);

## 6. **CRONOGRAMA FÍSICO E DE EXECUÇÃO**

Cada atividade é indicada por uma letra. O período de realização de uma atividade e a interdependência (anteriormente citada) entre elas pode ser facilmente observada nos cronogramas apresentados. Os períodos de revisão de uma atividade são indicados por um (\*). Quando o (\*) não aparecer, isto significa que a atividade somente será revisada no final (ao término de sua execução).

### **Atividades**

A	Refinamento e Validação de Políticas de Segurança e Segurança Multilateral	Carlos Becker Westphall Ricardo Felipe Custódio Carla Merkle Westphall Abderrahim Sekkaki Luis Marco Caceres Alvarez Alexandre Parra	UFSC UFSC UFSC Marrocos UFSC UFSC	Doutor Doutor Doutora Doutor Doutorando Graduando
B	Framework RBAC (Role Based Access Control) para Aplicações Web	Carlos Becker Westphall Luiz Carlos Zancanella Carla Merkle Westphall Abderrahim Sekkaki Luis Marco Caceres Alvarez Kátyra Kowalski Armanini Marcel Castilho	UFSC UFSC UFSC Marrocos UFSC Thermus UFSC	Doutor Doutor Doutora Doutor Doutorando Mestre Graduando

C	Autenticação fim-a-fim para o LDP(Label Distribution Protocol) na Arquitetura MPLS	Carlos Becker Westphall Carla Merkle Westphall Ricardo Felipe Custódio Edison Tadeu Melo Morvan Daniel Muller Leonardo N. Bernardo	UFSC UFSC UFSC UFSC Softplan UFSC	Doutor Doutora Doutor Mestre Mestre Graduando
D	IDS e Compartilhamento e Atualização de Bases de Assinaturas Utilizando Agentes Móveis	Carlos Becker Westphall Ricardo Felipe Custódio Fernando Augusto Cruz Luiz Nacamura Junior Alexandre Veloso Matos Guilherme Eliseu Rhoden Paulo Fernando da Silva	UFSC UFSC UFSC CEFFET-PR UFSC UFSC UFSC	Doutor Doutor Doutor Doutor Doutorando Mestre Mestrando
E	Aplicação de Inteligência Computacional (Lógica <i>Fuzzy</i> e Redes Neurais) na Gerência de Redes através da Automatização do uso de Agentes Móveis	Carlos Becker Westphall Sílvia Modesto Nassar Ricardo Felipe Custódio Arthur Ronald Buchsbaum Fernando Luiz Koch Juliana Amaral Arantes Edison Alessandro Xavier	UFSC UFSC UFSC UFSC Holanda UFSC UFSC	Doutor Doutora Doutor Doutor Doutorando Mestre Mestre
F	Arquitetura de <i>Grids</i> de Agentes Aplicada à Gerência de Redes	Carlos Becker Westphall Mario Dantas Fernando Luiz Koch Ana Lucia Anacleto Reis Tom Spindola Marcos Assunção Dias Cezar Bettoni Breno Syperrek Eduardo Erle Santos	UFSC UFSC Holanda FURB UFSC UFSC UFSC UFSC UFSC	Doutor Doutor Doutorando Mestre Mestre Mestrando Mestrando Mestre Graduando
G	Gerência de Redes em Ambientes WEB, WAP e SMS usando as Tecnologias SNMP, WBEM e CORBA	Carlos Becker Westphall Michele Sibilla Andre Melo Barotto André Barros Angela Melo Barotto Douglas Nazareno D. Vargas Gerson Valdir dos Santos Rodrigo Santana Sílvia C. C. Bianchi	UFSC França UFSC França UFSC UNIPLAC UFSC UFSC UFSC	Doutor Doutora Doutorando Doutorando Mestre Mestre Mestre Mestrando Graduanda
H	Gerência de Acordos de Níveis de Serviços para Redes Sem Fio	Carlos Becker Westphall Luiz Nacamura Junior Keith von Mecklenburg Júlio Cesar da Costa Ribas Abiel Roche Lima Mateus Casanova Pereira Madalena Pereira da Silva Rafael Tavares	UFSC CEFFET-PR Escócia CEFET-SC UFSC UFSC UFSC UFSC	Doutor Doutor Doutor Mestre Doutorando Mestrando Mestrando Graduando
I	Qualidade de Serviço (Perdas de pacotes, Latência e <i>Jitter</i> ) em Redes Sem Fio Ad Hoc	Carlos Becker Westphall Keith von Mecklenburg Júlio Cesar da Costa Ribas Abiel Roche Lima Gilson Norberto Horstmann Edivane Belle João Carlos Redin Michel Lobato	UFSC UFSC UFSC UFSC Embraco UFSC UFSC UFSC	Doutor Doutor Mestre Doutorando Mestre Mestre Mestrando Graduando
J	Reconhecimento de Padrões através de Redes Bayesianas e Algoritmo Genético Aplicado à Gerência de Segurança	Carlos Becker Westphall Sílvia Modesto Nassar Arthur Ronald Buchsbaum Fernando Augusto Cruz Rafael Plentz Luciana Pietroski	UFSC UFSC UFSC UFSC UFSC UFSC	Doutor Doutora Doutor Doutor Mestre Mestre

L	Aplicações de XML para Auxiliar na Gerência de Redes	Carlos Becker Westphall Carla Merkle Westphall Fabio Spanhol Eduardo Bueno Cleber V. Filippin Jean Pierre Ezequiel Júlio Alexandre de A. Reis	UFSC UFSC UNIOESTE UFSC UFSC UFSC UFSC	Doutor Doutora Mestre Mestrando Mestrando Mestrando Graduando
M	Gerenciamento de Serviços baseados em Políticas sobre Redes de Serviços Diferenciados	Carlos Becker Westphall Andre Melo Barotto Edison Tadeu Melo Richard R. Reinert Daniel Bitencourt Cadornin Aujor Tadeu Cavalca Andrade Fernanda Emanuella Silveira	UFSC UFSC UFSC UFSC UNISUL UFSC Thermus	Doutor Doutorando Mestre Mestre Mestre Mestrando Graduada
N	Licenças para Distribuição de Conteúdo Online em Sistemas DRM Usando a Linguagem XrML	Carlos Becker Westphall Carla Merkle Westphall Cleber V. Filippin Valério Rosset Daniel Quadros da Silva	UFSC UFSC UFSC UFSC UFSC	Doutor Doutora Mestrando Mestrando Graduando

Salienta-se que cada atividade apresenta uma instituição responsável, porém são realizadas com a colaboração ativa das demais instituições. Salienta-se também, que cada atividade é coordenada por um Doutor, e inclui na sua maioria, além dos pesquisadores em doutorado, candidatos a bolsa, colaboradores mestrando e graduando dos Cursos de Graduação e Pós-Graduação em Ciência da Computação.

#### Atividades previstas para execução e resultados esperados

##### Primeiro ano

	08/03	09/03	10/03	11/03	12/03	01/04	02/04	03/04	04/04	05/04	06/04	07/04
A			*			*			*			*
B			*			*			*			*
C			*			*			*			*
D			*			*			*			*
E			*			*			*			*
F			*			*			*			*
G			*			*			*			*
H			*			*			*			*
I			*			*			*			*
J			*			*			*			*
L			*			*			*			*
M			*			*			*			*
N			*			*			*			*
Todas												**

\* relatório de pesquisa, relatório de atividade e protótipos.

\*\* realização de *workshop* de avaliação do primeiro ano do projeto, com discussões que incluem as publicações das pesquisas realizadas em eventos internacionais da área.

##### Segundo ano

	08/04	09/04	10/04	11/04	12/04	01/05	02/05	03/05	04/05	05/05	06/05	07/05
A			*			*			*			*
B			*			*			*			*
C			*			*			*			*
D			*			*			*			*
E			*			*			*			*
F			*			*			*			*
G			*			*			*			*
H			*			*			*			*

I			*			*			*			*
J			*			*			*			*
L			*			*			*			*
M			*			*			*			*
N			*			*			*			*
Todas												**

\* relatório de pesquisa, relatório de atividade e protótipos finais.

\*\* realização de seminário com resultado de um livro com as pesquisas realizadas.

### Terceiro ano

	08/05	09/05	10/05	11/05	12/05	01/06	02/06	03/06	04/06	05/06	06/06	07/06
A			*			*			*			*
B			*			*			*			*
C			*			*			*			*
D			*			*			*			*
E			*			*			*			*
F			*			*			*			*
G			*			*			*			*
H			*			*			*			*
I			*			*			*			*
J			*			*			*			*
L			*			*			*			*
M			*			*			*			*
N			*			*			*			*
Todas												**

\* relatório de pesquisa, relatório de atividade e protótipos finais.

\*\* realização de seminário com resultado de um livro com as pesquisas realizadas.

## 7. DESCRIÇÃO MAIS DETALHADA DAS ATIVIDADES DE PESQUISA

Nesta seção as atividades de pesquisa a serem realizadas no projeto TAGERE serão mais detalhadas. Grande parte das atividades de pesquisa a serem desenvolvidas neste projeto TAGERE derivam de resultados do projeto anterior (Projeto HOPE – “Hot Topics” em Gerência de Redes). Para obter ainda mais embasamento sobre as atividades de pesquisa a serem desenvolvidas seria melhor consultar os resultados do projeto HOPE em [www.lrg.ufsc.br](http://www.lrg.ufsc.br). Inclusive um livro, em fase de edição, mostrando alguns resultados do projeto HOPE pode ser encontrado em [www.lrg.ufsc.br/hope/livro.pdf](http://www.lrg.ufsc.br/hope/livro.pdf).

### 7.1 Refinamento e Validação de Políticas de Segurança e Segurança Multilateral

#### 7.1.1 Introdução

A expansão dos sistemas abertos de comunicação e da Internet motiva o desenvolvimento de modelos de segurança que asseguram o fluxo correto de informações dentro de organizações públicas e privadas. Nestes sistemas abertos também é imprescindível considerar que ocorre a interação entre partes diferentes e cada uma dessas partes possui seus próprios requisitos de segurança.

O conceito de *segurança multilateral* visa um balanceamento entre os requisitos de segurança de diferentes partes ou entidades [Pfitzmann 2001, Rannenberg 2000], considerando todas as partes envolvidas em uma interação e ainda, que todas as entidades podem ser potenciais intrusos. O uso deste conceito pode ser visto e aplicado em ambientes de comércio eletrônico, com sistemas de pagamento de empresas interagindo com clientes e sistemas de cartões de crédito. Em sistemas de telecomunicações há a negociação entre características da provedora de serviço e necessidades do cliente. Para regular serviços de consultoria, há a interação entre empresa prestadora do serviço, empresa cliente do serviço e consultores responsáveis pela realização da tarefa.

Normalmente, a segurança multilateral é tratada na literatura de duas formas bem distintas. Na primeira [Pfitzmann 2001, Rannenberg 2000, Reichenbach et al 2000], considera-se que é necessário apenas haver a negociação entre partes de uma interação quanto aos requisitos de segurança que devem ser usados por todos em concordância. Na segunda visão sobre o assunto [Anderson 2001], modelos de segurança novos ou já existentes são utilizados para regular o aspecto da segurança multilateral.

Esta atividade apresenta um trabalho original e inédito, com o refinamento ou a reescrita das propriedades fundamentais do modelo de segurança *Chinese Wall* [Brewer e Nash 1989], considerando o conceito de segurança multilateral, com o objetivo de facilitar o seu entendimento e sua implementação. A atividade também implementa a política de segurança *Chinese Wall* considerando um ambiente comercial de consultoria de empresas.

Itens abordados: apresentação dos os conceitos básicos sobre segurança multilateral e sobre o modelo de segurança *Chinese Wall*; o refinamento ou reescrita das propriedades originais do modelo, e também a proposta de arquitetura usada para implementar o *Chinese Wall* em Java; esultados de implementação; e trabalhos relacionados.

### 7.1.2 Trabalhos em Andamento e Futuros

Esta atividade apresentou o *ChiWa*, uma proposta, implementação e validação de uma arquitetura de classes que concretiza a combinação do modelo de segurança *Chinese Wall* e de conceitos de segurança multilateral com o uso deste modelo.

O conceito de segurança multilateral está presente, mesmo que de forma não consciente, em ambientes de negócios. A exemplo do trabalho de [Foley 1997], o sistema *ChiWa* é uma implementação do modelo *Chinese Wall*. Porém, a implementação apresentada nesta atividade teve ainda como objetivo validar o conceito de segurança multilateral entre as seguintes partes: consultores, prestadora dos serviços de consultoria e as empresas onde os consultores atuam realizando serviços, usando o modelo de segurança *Chinese Wall*. Esta combinação entre segurança multilateral e o modelo *Chinese Wall* é um trabalho original e inédito que ainda não foi descrito na literatura técnico-científica.

O *ChiWa* apresenta contribuições na área de modelos de segurança que podem ser usados para o desenvolvimento de aplicações comerciais seguras. Contribui para um melhor entendimento da política de segurança *Chinese Wall*, e também da segurança multilateral entre os consultores, prestadora dos serviços de consultoria e as empresas onde os consultores atuam. Usando o *Chinese Wall*, a segurança multilateral é tratada de maneira fundamentada e formal no que diz respeito ao controle de acesso, diferente do trabalho de [Pfitzmann 2001, Pfitzmann et al 1998] que trata a segurança multilateral de maneira informal e considera apenas a negociação de requisitos de segurança entre as partes. O *Chinese Wall* possibilita o reconhecimento dos conflitos de segurança entre as partes e o tratamento desses conflitos através das propriedades simples e estrela.

Dentre as possibilidades de trabalhos futuros, pode-se citar o uso do CORBA para distribuir a aplicação comercial que necessita de segurança, ou seja, do *ChiWa*, e também da política de autorização definida no *ChiWa*. Uma idéia a ser investigada será a possibilidade de uso do *ChiWa* aperfeiçoado para controlar a venda de informações de *sites* de vários países, considerando: as leis próprias de cada um dos países onde estes *sites* residem, a interação entre as várias partes e a segurança multilateral usando o *Chinese Wall*.

### 7.1.3 Referências Bibliográficas

- [Anderson 2001] Anderson, Ross. Security Engineering – A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.
- [Bell e Lapadula 1976] Elliot Bell, D. e LaPadula, Leonard J. (1976) "Security Computer Systems: Unified Exposition and Multics Interpretation", MITRE Tech. Report MTR-2297 Rev. 1, MITRE Corporation, Bedford, MA, March 1976.
- [Brewer e Nash 1989] Brewer, D. F. C. e Nash, M. J. "The Chinese Wall Security Policy", In: Proceedings of the 1989 IEEE Symposium on Security and Privacy, p. 206-214, Oakland, California, 1989.
- [Clark e Wilson 1987] Clark, D. R., e Wilson, D. R. "A Comparison of Commercial and Military Computer Security Policies", In: Proceedings of the 1987 IEEE Symposium on Security and Privacy, p. 184-194, Oakland, California, 1987.
- [Foley 1997] Foley, S. "Building Chinese Walls in standard Unix", Computers and Security Journal, 16(6):551 -563, December 1997.
- [Gollmann 1999] Gollmann, Dieter. Computer Security, John Wiley and Sons, 1999.
- [Investor 2002] Site InvestorWords. "Chinese Wall", <http://www.investorwords.com/cgi-bin/getword.cgi?854>, 2002.
- [Larman 2000] Larman, Craig. Utilizando UML e Padrões: Uma introdução à análise e ao projeto orientados a objetos, Editora Bookman, 2000.
- [McLean 1987] McLean, John. "Reasoning About Security Models", In: Proceedings of the 1987 IEEE Symposium on Security and Privacy, p. 123-131, Oakland, California, 1987.
- [Pfitzmann 2001] Pfitzmann, A. "Multilateral Security: Enabling Technologies and Their Evaluation", In: Lecture Notes in Computer Science 2000, edited by R. Wilhelm, Informatics: 10 Years Back. 10 Years Ahead, 2001, p. 50-62.

- [Pfitzmann et al 1998] Pfitzmann, A., Schill, A., Westfeld, A., Wicke, G., Wolf, G. e Zöllner, J. "A Java-based distributed platform for multilateral security", In: IFIP/G1 Working Conference – Trends in Electronic Commerce, Lectures Notes in Computer Science 1402, 1998, p. 52-64.
- [Rannenber 2000] Rannenber, Kai. "Multilateral Security - A concept and examples for balanced security", In: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, 19–21 September 2000 Cork, Ireland, ACM Press, p. 151-162.
- [Reichenbach et al 2000] Reichenbach, M., Grzebiela, T., Költzsch, T., e Pippow, I. "Individual Risk Management for Digital Payment Systems". In: Hansen, H.-R.; Bichler, M.; Mahrer, H. (2000): Proceedings of the 8<sup>th</sup> European Conference on Information Systems (ECIS), Wien, p. 875-882, 2000.
- [Sandhu 1993] Sandhu, Ravi S. "Lattice-based access control models", IEEE Computer, v. 26, n. 11, p. 9-19, November 1993.
- [Sun 2002a] Sun Microsystems Inc. The Java Tutorial – A practical guide for programmers, Tutorial, <http://java.sun.com/docs/books/tutorial/index.html>, 2002.
- [Sun 2002b] Sun Microsystems Inc. Java 2 Platform – Standard Edition, v. 1.4.1, <http://java.sun.com/j2se/1.4.1/index.html>, October 2002.
- [Wayman 2001] Rick Wayman. "What is the "Chinese Wall" and Why is it in the News?", <http://www.investopedia.com/articles/analyst/090501.asp>, 2001.
- [Westphall 2000] Westphall, Carla Merkle. Um esquema de Autorização para a Segurança em Sistemas Distribuídos de Larga Escala, Tese de Doutorado, Curso de Pós-Graduação em Engenharia Elétrica, UFSC, Dezembro 2000.

## 7.2 Framework RBAC (Role Based Access Control) para Aplicações Web

### 7.2.1 Introdução

Com a utilização cada vez maior da Internet e das Intranets dentro das empresas, o crescimento do uso de aplicações Web se torna inevitável. Considerando que em uma empresa existem funcionários com atividades e funções diferentes, onde alguns possuem mais privilégios que outros, existe a necessidade de controlar os privilégios dos funcionários na utilização das aplicações Web da empresa. As principais preocupações com relação à segurança são a confidencialidade, as informações só são reveladas para pessoas autorizadas; integridade, a informação só pode ser modificada por funcionários autorizados das maneiras autorizadas; responsabilidade, funcionários são responsáveis por suas ações relacionadas à segurança; e acessibilidade (disponibilidade), funcionários autorizados não podem ter seu acesso negado maliciosamente.

Além disso, com o crescimento das empresas ocorreu um aumento do volume de informação e do número de funcionários, e conseqüentemente os problemas de segurança cresceram e se tornaram mais difíceis [OH 00]. O controle de acesso por si só não é uma solução completa para obtenção de segurança em um sistema. Para que a segurança seja completa, é necessária a existência de outros serviços de segurança como autenticação, auditoria e administração [SANDHU 94]. A autenticação é para garantir que um usuário é quem ele diz ser; controles de acesso, para controlar o que um usuário pode acessar em um sistema; comunicações seguras, para proteger informações em trânsito entre componentes; auditoria de segurança, para gravar e analisar o que o usuário faz no sistema; e administração de segurança, para gerenciar informações de segurança incluindo as políticas de segurança.

De acordo com um estudo do NIST (*National Institute of Standards and Technology*), essa necessidade de controles de acesso de acordo com os papéis que os usuários e ou funcionários individualmente desempenham na organização define uma política de segurança denominada de RBAC (*Role-Based Access Control*), ou seja, um modelo de segurança baseado em papéis [WESTPHALL 00]. O *Role Based Access Control* (RBAC) é um termo utilizado para descrever políticas de segurança que controlam o acesso de usuários a recursos computacionais, baseado na construção de roles (papéis, funções). Esses papéis definem um conjunto de atividades concedidas para usuários autorizados. Pode-se imaginar um papel como se fosse um cargo ou posição dentro de uma organização, que representa a autoridade necessária para conduzir as tarefas associadas. Para muitos tipos de organização, o modelo RBAC fornece um modo mais intuitivo e eficaz de representar e gerenciar autorizações às informações que outras formas de controle de acesso [JANSEN 98][OH 00].

Outra motivação deste trabalho é a reusabilidade de componentes, que atualmente é reconhecida como uma forma importante de aumentar a produtividade no desenvolvimento de software. Os programadores com mais experiência em sua maioria já reutilizam código e consultam códigos antigos, mas o potencial de reutilização das partes de análise e projeto de um sistema ainda é pouco explorado [LANDIN 95].

Dentro deste contexto existe o conceito de *frameworks*, que torna possível não somente a reutilização de código, mas também da parte de análise e projeto [LANDIN 95]. Um *framework* nada mais é do que uma estrutura de classes inter-relacionadas, que corresponde a uma implementação incompleta para um conjunto de

aplicações de um domínio. Esta estrutura de classes deve ser adaptada para a geração de aplicações específicas [SILVA 00].

Observando este cenário, o objetivo deste trabalho é a criação de um *framework* baseado no modelo de segurança RBAC e que possa ser utilizado por aplicações Web. Este *framework* é composto por várias classes (concretas e abstratas) que implementam mecanismos de autenticação, controle de acesso, auditoria e administração. A utilidade deste *framework* está na diminuição do tempo de desenvolvimento da parte de segurança de aplicações Web ou de aplicações Java que utilizem a política de papéis.

Como o propósito deste *framework* é para ser utilizado principalmente por aplicações com interface Web, a linguagem de implementação escolhida foi Java e o item de segurança de comunicação segura omitido, já que no ambiente proposto este item é garantido pelo protocolo SSL (*Secure Socket Layer*), o qual já se encontra implementado na maioria dos servidores Web existentes no mercado. Nada impede que a especificação do *framework* seja utilizada para implementação em outra linguagem de programação e seja utilizada para qualquer tipo de aplicação que queira adotar o modelo de segurança RBAC. Neste caso, é sugerido que haja uma preocupação com relação à parte de comunicação segura.

Este trabalho aborda: política de segurança RBAC, descrevendo os elementos e regras do mesmo; apresenta o conceito de *framework* e os aspectos que caracterizam o mesmo; e apresentada a estrutura do *framework* desenvolvido e como foram implementadas as regras do modelo RBAC dentro do *framework*.

### 7.2.2 Trabalhos em Andamento e Futuros

As principais contribuições deste trabalho:

1. O projeto e implementação de um *framework* baseado no modelo de segurança RBAC, que também dá suporte à autenticação, auditoria, administração e persistência das informações de segurança;
2. A utilização de padrões de projeto na implementação de *framework* RBAC, o que permitiu a implementação de técnicas como a materialização sob demanda, fazendo com que apenas informações que serão utilizadas sejam carregadas para a memória;
3. A definição de um modelo de dados para o armazenamento das informações dos elementos do modelo de segurança RBAC em uma base de dados, e que também dá suporte à implementação das regras deste modelo;
4. A proposta de um modo de implementação das regras do modelo RBAC.

Continuidade deste trabalho: A principal continuidade é a evolução da estrutura do *framework*, onde poderão ser incluídas novas funcionalidades, de acordo com a necessidade dos desenvolvedores que irão utilizá-lo. Um exemplo de evolução é o aprimoramento do esquema de autenticação, que poderia ser estendido para a utilização de chaves públicas, já que atualmente o *framework* só permite a utilização de senhas e chaves privadas. A parte de auditoria também poderia ser melhorada, no sentido de ser melhor analisada e projetada, com o objetivo de facilitar seu uso.

Outro trabalho que será realizado é a implementação da camada de persistência utilizando arquivos textos ou banco de dados orientados a objetos para o armazenamento das informações de segurança.

### 7.2.3 Referências Bibliográficas

[BROWN 96] BROWN, K. WHITENACK, B. Crossing Chasms. Pattern Languages of Program Design. 1996. vol. 2. Reading, MA. Editora: Addison-Wesley.

[BUNDY 01] BUNDY, Alan; BLEWITT, Alex; STARK, Ian. Automatic Verification of Java Design Patterns. Division of Informatics. University of Edinburgh. IEEE- Automated Software Engineering, 2001. (ASE 2001). Proceedings. 16th Annual International Conference on, 2001. Pg. 324-327.

[FERRAILOLO 95] FERRAILOLO, David F.; CUGINI, Janet A.; KUHN, D. Richard. Role-Based Access Control (RBAC): Features and Motivations. 1995. U. S. Department of Commerce. NIST – National Institute of Standards and Technology.

[FERRAILOLO 99] FERRAILOLO, David F.; BARKLEY, John F., KUHN, D. Richard. A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet. 1999. NIST – National Institute of Standards and Technology.

[GAMMA 95] GAMMA, Erich; HELM, Richard; JOHNSON, Ralph; VLISSIDES, John. Design Patterns: Elements of Reusable Object-Oriented Software. 1994. Reading: Addison-Wesley.

[JANSEN 98] JANSEN, W. A. A Revised Model for Role-Based Access Control. 1998. NIST 6192.

[LANDIN 95] LANDIN, Nicklas; NIKLASSON, Axel. Development Of Object Oriented Frameworks. 1995. Ericsson Software Technology.

[LARMAN 00] LARMAN, Craig. Utilizando UML e Padrões: Uma Introdução à Análise e Ao Projeto Orientado a Objetos. 2000. Porto Alegre. Editora Bookman.

[MENS 01] MENS, Tom; TOURWÉ, Tom. A Declarative Evolution Framework for Object-Oriented Design Patterns. 2001. Programming Technology Lab. Vrije Universiteit Brussel. Belgium. Software Maintenance, 2001. Proceedings. IEEE International Conference on , 2001 .Pg 570 –579.

[OBELHEIRO 02] OBELHEIRO, Rafael Rodrigues; FRAGA, Joni S. Role-Based Access Control for CORBA Distributed Object Systems. 2002. Departamento de Automação e Sistemas. Universidade Federal de Santa Catarina. IEEE - Object-Oriented Real-Time Dependable Systems, 2002. (WORDS 2002). Proceedings of the Seventh International Workshop on , 2002 Pg: 53 –60.

[OH 00] OH, Sejong; PARK, Seog. Enterprise Model as a Basis of Administration on Role-Based Access Control. Dept. of Computer Science, Sogang University , Seoul, Korea. IEEE – Cooperative Database Systems for Advanced Applications, 2001, CODAS 2001. The Proceedings of the Third International Symposium on 2000. Pg. 150-158.

[PAPA 00] PAPA, M.; BREMER, O.; CHANDIA, R.; HALE, J.; SHENOI, S. Extending Java for Package Based Access Control. Center for Information Security. Department of Computer Science, Keplinger Hall. University of Tulsa, Oklahoma. Computer Security Applications, 2000. ACSAC'00. 16<sup>th</sup> Annual Conference 2000. Pg. 67-76.

[SANDHU 94] SANDHU, Ravi; SAMARATI, Pierangela. Access Control: Principle and Practice. IEEE Communications Magazine, Volume 32 Issue: 9 Sept. 1994. Pg. 40-48.

[SANDHU 98] SANDHU, Ravi; MUNAWER, Qamar. The RBAC97 Model for Role-Based Administration of Role Hierarchies. Laboratory for Information Security Technology (LIST) and ISE Department. George Mason University. IEEE - Computer Security Applications Conference, 1998. Proceedings. 14<sup>th</sup> Annual, 1998. Pg. 39-49.

[SANDHU 99] SANDHU, Ravi; MUNAWER, Qamar. The ARBAC99 Model for Administration Roles. Laboratory for Information Security Technology (LIST) and ISE Department. George Mason University. IEEE - Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15<sup>th</sup> Annual, 1999. Pg. 229-238.

[SILVA 00] SILVA, Ricardo Pereira e. Suporte ao Desenvolvimento e Uso de Frameworks e Componentes. 2000. Tese de Doutorado. Programa de Pós-Graduação em Computação. Universidade Federal do Rio Grande do Sul.

[WESTPHALL 00] WESTPHALL, Carla Merkle. Um Esquema de Autorização para a Segurança em Sistemas Distribuídos de Larga Escala. 2000. Curso de Pós-Graduação em Engenharia Elétrica da UFSC.

### 7.3 Autenticação fim-a-fim para o LDP(Label Distribution Protocol) na Arquitetura MPLS

#### 7.3.1. Introdução

O MPLS (*Multiprotocol Label Switching*), conforme a RFC3031 [ROSEN, 2001], é um *framework* definido pelo IETF (*Internet Engineering Task Force*) que proporciona designação, encaminhamento e comutação eficientes de fluxos de tráfego através da rede, por ser uma técnica de comutação de pacotes baseada em etiquetas (*labels*). Na arquitetura MPLS, o protocolo LDP (*Label Distribution Protocol*) é responsável pela distribuição das etiquetas e pelo estabelecimento de caminhos lógicos chamados LSPs (*Label Switched Paths*). Estes caminhos lógicos são criados por roteadores LSRs (*Label Switched Routers*) interligados entre si.

Como o LDP exerce uma função primordial dentro do ambiente MPLS, uma lacuna na segurança do LDP pode comprometer todo o ambiente, tendo em vista que a distribuição das etiquetas (*labels*), realizada pelo LDP, é o que determina quem pode participar ou não do domínio MPLS. A forma de autenticação definida para o LDP [ANDERSSON, 2001], está restrita a LSRs adjacentes e depende de uma conexão TCP entre os LSRs envolvidos. Sendo assim, esta solução não trata situações em que dois LSRs, não-adjacentes, pretendem se autenticar mutuamente fim a fim, durante o estabelecimento de um novo LSP.

Desta forma, este trabalho propõe uma solução de autenticação fim a fim para o protocolo LDP, de modo a preencher esta lacuna do protocolo, viabilizando o estabelecimento de LSPs entre dois LSRs não-adjacentes. A solução de autenticação fim a fim, foi planejada para ambientes onde LSPs atravessam múltiplos domínios externos, considerados não confiáveis, e que por isso necessitam se autenticar durante o estabelecimento de um novo LSP. *Conforme foi verificado pelo levantamento de trabalhos correlatos [DE CLERCQ, 2001], [BUDA, 2001], [KENT, 2000], [BADAN, 2001], atualmente é desconhecida uma solução de autenticação semelhante, que*

*efetivamente atenda o propósito de autenticar num escopo fim a fim, o estabelecimento de LSPs dentro do protocolo LDP. Dessa forma a solução proposta por este trabalho é inédita dentro do seu escopo de aplicação.*

Este trabalho aborda: descreve sucintamente como ocorre o processo de distribuição de etiquetas no MPLS; apresenta algumas características do funcionamento do protocolo LDP; faz considerações sobre Requisitos de Segurança para o LDP e apresenta alguns trabalhos relacionados; e a proposta de autenticação fim a fim para o LDP é descrita.

### **7.3.2 Trabalhos em Andamento e Futuros**

Este trabalho apresentou uma solução de autenticação para o protocolo LDP, de forma a viabilizar uma autenticação fim a fim, entre um LSR de ingresso e seu respectivo LSR de egresso durante o estabelecimento de um novo LSP. Conforme verificado pelo levantamento dos trabalhos relacionados apresentados, não se tem conhecimento de uma solução semelhante, que efetivamente atenda o propósito de autenticar, num escopo fim a fim, o estabelecimento de LSPs entre LSRs não-adjacentes no protocolo LDP. Dessa forma a solução deste trabalho é inédita dentro do seu escopo de aplicação.

Conclui-se que a solução de autenticação fim a fim para o protocolo LDP, apresentada neste trabalho, trouxe incrementos importantes que vem a suprir lacunas e deficiências dentro da atual especificação deste protocolo, especialmente com relação a segurança do ambiente. Uma forma de autenticação fim a fim, para viabilizar a autenticação mútua entre os LSRs de ingresso e egresso durante o estabelecimento de um LSP, é de fundamental importância para a segurança do protocolo LDP, especialmente dentro de ambientes MPLS multi-domínios, onde os domínios não são confiáveis entre si. Pôde-se constatar através da implementação realizada na plataforma Linux, que este objetivo foi prontamente atendido pela proposta de autenticação apresentada.

Como um exemplo clássico de ambientes multi-domínio, temos o provimento de VPNs baseadas em BGP/MPLS, em ambientes multiprovedores VPN, retratado em [ROSEN, 1999] e [ROSEN, 2002], onde vários provedores VPN fornecem o serviço VPN baseados em acordos que possuem entre si. Embora não comprovado por um experimento prático, como uma implementação, a solução de autenticação apresentada neste trabalho pode ser perfeitamente aplicada ao protocolo CR-LDP, visto que o mesmo teve sua concepção baseada no LDP.

Em comparação aos trabalhos correlatos discutidos, a solução apresentada por [DE CLERCQ, 2001] possui em níveis gerais os mesmos objetivos da proposta deste trabalho. Através de uma análise aprofundada da proposta de [DE CLERCQ, 2001], conclui-se que a mesma apresenta um erro arquitetural, fato reconhecido pelos seus autores através de contato por e-mail. Por considerar erroneamente, que ao enviar uma mensagem solicitando o estabelecimento de um LSP para uma determinada FEC, o LSR de origem sabe qual é o LSR de destino que vai processar a requisição, o escopo de aplicação da solução dentro do LDP fica drasticamente reduzido.

Em contrapartida, a solução de autenticação apresentada neste trabalho atende a todas as situações de estabelecimento de LSPs entre LSRs no LDP, embora sua principal aplicabilidade seja em comunicações entre LSRs não-adjacentes.

Este trabalho será continuado através de:

- a) Especificar mais detalhadamente e implementar a distribuição de chaves usando certificação digital.
- b) avaliar os prós e contras de prover confidencialidade as informações transportadas pelo protocolo LDP. Existem opiniões que divergem neste sentido, dessa forma seria justificável um estudo aprofundado. Caso conclua-se vantajosa a adoção de confidencialidade no ambiente, sugere-se a especificação de uma solução que atenda as necessidades levantadas pelo estudo de viabilidades realizado.
- c) analisar e propor as modificações necessárias na proposta de autenticação fim a fim apresentada neste trabalho, de modo a fornecer suporte a IP Versão 6 (ipv6). Não serão necessárias grandes mudanças para atingir este propósito, porém este objetivo não estava incluso no escopo do corrente trabalho, dessa forma ficou pendente para revisões futuras.

### **7.3.3 Referências Bibliográficas**

ABADI, M.; NEEDHAM, R. Prudent Engineering. Practice for Cryptographic Protocols. IEEE Transactions on Software Engineering, v. 22, n. 1, p. 6-15, 1996. Disponível por <http://www.cs.virginia.edu/~survive/DOCS/prudent.ps>. Acesso em 10 set. 2002.

Ayame Project – MPLS Implementation for NetBSD. Início das atividades em outubro de 1999. Disponível por <http://www.ayame.org/AYAMEproject.php>. Acesso em 9 Mai. 2002.

ANDERSSON, L.; Doolan, P., Feldman, N., et al. LDP Specification. RFC 3036, janeiro de 2001. Disponível por <http://www.ietf.org/rfc/rfc3036.txt>. Acesso em 20 nov. 2001.

AWDUCHE, D; BERGER, L RSVP-TE: Extensions to RSVP for LSP Tunnels. RFC 3209, dezembro de 2001. Disponível por <http://www.ietf.org/rfc/rfc3209.txt>. Acesso em 25 mar. 2002.

BADAN, Tomás. A. C.; PRADO, Rodrigo C. M.; ZAGARI, Eduardo N. F.; et. al. Uma Implementação MPLS para Redes Linux. Universidade de Campinas (UNICAMP), DCA – FEEC. Publicado no SBRC 2001, maio de 2001. Disponível por <http://www.sbrc2001.ufsc.br/artigos/4807-7171.pdf>. Acesso em 15 abr. 2002.

BUDA, G.; CHOI, D.; et. al. Security Standarts for the Global Information Grid. IEEE, 0-7803-7272-1/01, 2001.

DE CLERCQ, J.; PARIDAENS, O.; T'JOENSET Y., SCHRIJVER, P. End to End Authentication for LDP. Draft-schrijvp-mpls-ldp-end-to-end-auth-03.txt. [jeremy.de\\_clercq@alcatel.be](mailto:jeremy.de_clercq@alcatel.be), fevereiro de 2001. Contato com o author em 10 jan. 2002. A Draft expirou, cf.. <http://www.ietf.org/internet-drafts/draft-schrijvp-mpls-ldp-end-to-end-auth-04.txt>.

HEFFERNAN, A. Protection of BGP Sessions via the TCP MD5 Signature Option. Draft-ietf-idr-rfc2385bis-00.txt, março de 2002. Disponível por <http://www.ietf.org/internet-drafts/draft-ietf-idr-rfc2385bis-01.txt>. Acesso em 19 mar. 2002. (Trabalho em progresso).

KENT, S.; LYNN, C.; SEO, K. Secure Border Gateway Protocol (S-BGP). IEEE Journal on Selected Areas In Communications, VOL. 18, NO. 4, abril de 2000.

LEU, J; et. al. Project: MPLS for Linux. Início das atividades em 27 de novembro de 2000. Disponível por <http://sourceforge.net/projects/mpls-linux>. Acesso em 06 fev. 2002. (Trabalho em progresso).

MAGALHÃES, M. F.; CARDOZO, E. Introdução a Comutação ao IP por Rótulos Através de MPLS. Universidade de Campinas (UNICAMP), DCA – FEEC. Publicado no SBRC 2001, Minicursos, maio de 2001.

NEEDHAM, R.; ABADI, M. Prudent Engineering Practice for Cryptographic Protocols. IEEE Transactions on Software Engineering, v. 22, n. 1, p. 6-15, 1996. Disponível por <http://www.cs.virginia.edu/~survive/DOCS/prudent.ps>. Acesso em 10 ago. 2002.

NIST - *National Institute for Standards and Technology*. Descriptions of SHA-256, SHA-384, and SHA-512. Outubro de 2000. Disponível por <http://csrc.nist.gov/cryptval/shs/sha256-384-512.pdf>. Acesso em 20 mai. 2002.

REKHTER, Y; ROSEN, E. Carrying Label Information in BGP-4. RFC 3107, maio de 2001. Disponível por <http://www.ietf.org/rfc/rfc3107.txt>. Acesso em 22 jan. 2002.

ROSEN, E.; REKHTER, Y. BGP/MPLS VPNs. Draft-ietf-ppvpn-rfc2547bis-02, julho de 2002. Disponível por <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-rfc2547bis-02.txt>. Acesso em 08 ago. 2002.

ROSEN, E.; TAPPAN, D.; FEDORKOW, G., et al. MPLS Label Stack Encoding. RFC 3032, janeiro de 2002a. Disponível por <http://www.ietf.org/rfc/rfc3032.txt>. Acesso em 12 set. 2001.

ROSEN, E; VISWANATHAN, A.; CALLON, R. Multiprotocol Label Switching Architecture. RFC 3031, janeiro de 2001. Disponível por <http://www.ietf.org/rfc/rfc3031.txt>. Acesso em 26 jul. 2001

## **7.4 IDS e Compartilhamento e Atualização de Bases de Assinaturas Utilizando Agentes Móveis**

### **7.4.1. Introdução**

Sistemas de detecção de intrusão (*Intrusion Detection Systems – IDS's*) são ferramentas utilizadas na tentativa de identificação e rastreamento de ataques a redes de computadores. Diversas técnicas são aplicadas a estes sistemas na busca de uma maior eficiência na detecção de ataques. Algumas das técnicas mais conhecidas são: análise de assinaturas, sistemas adaptativos e análise estatística. Destas técnicas, a mais utilizada é a análise de assinaturas.

Os IDS's baseados na técnica de análise de assinaturas utilizam uma base de dados contendo várias seqüências de eventos, chamadas de assinaturas. Estes IDS's consistem na monitoração de eventos da rede ou *hosts* em que estão instalados, tentando identificar se os eventos que estão ocorrendo no sistema correspondem a alguma das assinaturas cadastradas na base de dados. Se o IDS encontrar uma seqüência de eventos no sistema que corresponda a uma assinatura da base de dados, então possivelmente estará ocorrendo um ataque ao sistema, e o IDS irá tomar alguma providência para conter este ataque. Esta providência pode ser um alerta sonoro ou visual no computador que está sendo atacado, o envio de um E-mail para o administrador da rede, ou até mesmo a interrupção da conexão ou do processo que está causando o ataque.

Dentre os problemas encontrados nos sistemas de detecção de intrusão baseados em análise de assinaturas podemos citar a dificuldade de se manter atualizada a base de assinaturas e a falta de padrão entre

as assinaturas dos diferentes IDS's existentes. Atualmente a atualização da base de assinaturas é feita de forma manual, exigindo conhecimento do usuário sobre a sintaxe das assinaturas em um IDS específico. Outra forma de atualização da base de assinaturas é através de atualizações disponibilizadas pelos fabricantes dos IDS's, esta forma de atualização exige que o usuário substitua periodicamente a sua base de assinaturas local pela base disponibilizada pelo fabricante.

O trabalho refere-se a comunicação, troca de informações e cooperação entre os diferentes IDS's existentes no mercado. Este trabalho propõe uma arquitetura para que os diferentes IDS's trabalhem em conjunto, compartilhando as suas bases de assinaturas e atualizando-as de forma automática, aumentando assim a eficiência destas ferramentas. Para isto a arquitetura proposta define uma estrutura para o armazenamento das assinaturas, esta estrutura é utilizada nas bases de assinaturas que são compartilhadas entre os IDS's.

Para realizar a troca de informações entre os IDS's, foi utilizada a tecnologia de agentes móveis. Agentes Móveis são programas cujo código de execução possui recursos capazes de armazenar dados, transferir-se de um local para outro da rede e reiniciar sua execução. A recuperação de informação e o comércio eletrônico são suas principais áreas de aplicação. Algumas das tarefas realizadas por agentes móveis são a busca de informações na rede e a execução de tarefas distribuídas.

Optou-se pela utilização de agentes móveis devido às suas características, principalmente no que diz respeito à recuperação de informações distribuídas. Este estudo demonstra que os agentes móveis são pouco influenciados por gargalos na rede, esta característica pode ser importante em um ambiente como a Internet.

A plataforma de agentes móveis escolhida foi a plataforma Java Aglets. O Aglet é um agente móvel Java que suporta os conceitos de execução autônoma e roteamento dinâmico em seu itinerário. Os Aglets são hospedados por um servidor Aglet de forma similar à forma como os applets são hospedados por um Web browser. O servidor Aglet provê um ambiente para os aglets executarem e uma máquina virtual Java que, juntamente com o gerenciador de segurança do Aglet, tornam este servidor seguro para receber e hospedar os Aglets.

Cada um dos IDS's que faz parte da arquitetura de compartilhamento e atualização de bases de assinaturas irá publicar uma base de assinaturas contendo as suas assinaturas armazenadas dentro do formato padrão definido pela arquitetura. Os agentes móveis irão navegar pela rede em busca de novas assinaturas, visitando as bases de assinaturas que foram publicadas.

Quando um agente móvel encontra uma assinatura nova, ele retorna ao IDS que o disparou e atualiza a sua base de assinaturas. Desta forma a base de assinaturas do IDS estará sempre atualizada, de forma automática, eliminando a preocupação do usuário em ficar constantemente atualizando sua base.

O objetivo geral deste trabalho consiste em desenvolver uma arquitetura que proporcione a atualização automática da base de assinaturas de um IDS. Esta atualização será feita através de agentes móveis que realizam consultas em bases de assinaturas de outros IDS's, espalhadas pela Internet.

Como objetivos específicos temos:

- desenvolvimento de uma estrutura para o armazenamento das assinaturas;
- desenvolvimento de uma estrutura para publicação da base de assinaturas, de forma a possibilitar a consulta destas assinaturas;
- desenvolvimento de agentes móveis capazes de consultar e copiar assinaturas de bases publicadas por IDS's;

Além disto este trabalho visa apresentar: as justificativas e motivações que levaram à realização deste trabalho, citando alguns trabalhos correlatos; detalhes da metodologia e do ambiente de desenvolvimento utilizados; a estrutura para armazenamento das assinaturas; e a arquitetura de compartilhamento e atualização respectivamente.

#### **7.4.2 Trabalhos em Andamento e Futuros**

Atualmente, para se atualizar uma base de assinaturas um usuário precisa conhecer os novos ataques e assinaturas que são criados todos os dias, analisar estas novas assinaturas e verificar se elas são necessárias dentro da rede específica em que trabalha e, atualizar manualmente a base de assinaturas de sua rede se for o caso. Como ataques e assinaturas são criadas constantemente, e a atualização das bases ainda é feita de forma bastante manual, são grandes as chances da base de assinaturas de uma empresa não estar totalmente atualizada e ser surpreendida por um ataque recém criado ou uma vulnerabilidade recém descoberta, sem que o IDS tenha consciência de que isto está ocorrendo.

A atualização também pode ser feita diretamente pelo fabricante de um IDS específico. Porém nestes casos todos os usuários do IDS daquele fabricante recebem a mesma base de assinaturas, ou seja, a base não é otimizada de acordo com as realidades e necessidades de cada rede. A base enviada pelo fabricante pode não satisfazer as necessidades específicas de uma rede, obrigando o usuário a novamente configurar e atualizar a sua base de assinaturas de forma manual.

A contribuição do presente trabalho para com a segurança das redes de computadores vem através da possibilidade de atualização automática e eficiente das bases de assinaturas, eliminando a necessidade de um

usuário realizar este trabalho manualmente. A arquitetura para compartilhamento e atualização de bases de assinaturas através de agente móveis apresentada neste artigo abre caminho para esta possibilidade.

A arquitetura possibilita que um IDS atualize a sua base de assinaturas de forma automática. Um usuário pode configurar que tipo de assinaturas interessa para sua rede e, com base nesta configuração agentes móveis realizam pesquisas nas bases de assinaturas de outras redes. A pesquisa é feita em diversas bases de outras redes, inclusive bases não conhecidas pela rede de origem, isto permite que uma base de assinaturas que utilize a arquitetura proposta seja alimentada com informações de várias fontes, e não somente de uma fonte central como no caso de uma base distribuída por um fabricante de IDS.

A possibilidade de configurar as características das assinaturas a serem pesquisadas garante que a base de assinaturas, que está sendo atualizada automaticamente, esteja sempre com informações (assinaturas) que esteja de acordo com as realidades e necessidades da rede em questão.

A arquitetura desenvolvida e apresentada neste trabalho permite que os sistemas de detecção de intrusão, baseados na técnica de análise de assinaturas, tornem-se ferramentas mais eficientes no auxílio à segurança das redes de computadores. A arquitetura apresentada aumenta a eficiência do sistema devido a possibilidade da troca de informações e da cooperação entre diferentes IDS's.

Vários aperfeiçoamentos podem ser aplicados à arquitetura apresentada neste artigo, a fim de torna-la mais robusta, confiável e eficaz.

Um dos aspectos que poderia ser trabalhado nesta arquitetura é a questão da integridade das bases de assinaturas. No presente trabalho quando um agente móvel pesquisa uma base de assinaturas remota, ele considera que esta base contém informações corretas e confiáveis. Porém, alguém interessado em prejudicar a distribuição das assinaturas ou interessado em espalhar assinaturas falsas, poderia alterar de forma maliciosa uma base de assinaturas confiável, desta forma os agentes começariam a coletar assinaturas que prejudicariam o funcionamento de seus IDS's. Sendo assim, faz-se necessário algum mecanismo que possibilite o agente móvel conferir a integridade da base de assinaturas, antes de começar a pesquisar as assinaturas da base.

Outro aperfeiçoamento aplicável a este trabalho, seria dotar os agentes móveis de uma maior inteligência na busca das assinaturas e na escolha da próxima base a ser pesquisada. Esta inteligência teria como objetivo maximizar a busca por novas assinaturas, tentando evitar que o agente pesquise assinaturas que ele, de alguma forma, poderia saber que não são novas. A escolha da próxima base a ser pesquisada também poderia ser otimizada, evitando que o agente pesquise novamente uma base de assinaturas que já foi pesquisada recentemente.

Além das extensões aplicadas a arquitetura desenvolvida neste trabalho, podem ser desenvolvidos trabalhos aplicando as idéias contidas nesta arquitetura a outras tecnologias. Pode-se tentar desenvolver uma arquitetura semelhante utilizando-se SNMP ou Web Services, ou ainda utilizando-se outras plataformas de agentes móveis.

### 7.4.3 Referências Bibliografia

- Arantes, J. A.; Westphall, C.B.; Custódio, R. F. (2002) "Modelo Analítico para Avaliar Plataformas Cliente/Servidor e Agentes Móveis Aplicado à Gerência de Redes". Anais do 20 Simpósio Brasileiro de Redes de Computadores (Vol. I). Búzios (RJ), p. 424-439.
- Buchheim, Tim, Erlinger, Michael, et al. (1999) "Implementing the intrusion detection exchange protocol", IEEE Computer Society.
- (2002) "CIFT – Common Intrusion Detection Framework", <http://gost.isi.edu/cidf/>, Outubro.
- (2002) "IBM Tokyo Research Laboratory", <http://www.trl.ibm.co.jp/aglets>, Outubro.
- (2002) "IETF – Internet Engineering Task Force", <http://www.ietf.org>. Outubro.
- Kahn, Cliffordn, Porras, Phillip, et al. (1998) "A common intrusion detection framework", Journal of Computer Security.
- Ning, Peng, Wang, Sean X., Jajodia, Sushil. (2000) "Modeling requests among cooperating intrusion detection", Computer Communications 23(17):1702-1715.
- Ning, Peng, Wang, Sean X., Jajodia, Sushil. (2001) "Abstraction-based Intrusion Detection in Distributed Environments", In ACM Transactions on Information and System Security, ACM Press.
- Pouzol, Jean P., Ducassé M. (2002) "Formal specification of intrusion signatures and detection rules", Proceedings of the 15th ComputerIEEE Computer Security Foundations Workshop. IEEE Computer Society Press.
- Schnackenberg, Dan, Djahandari, Kelly, et al. (2001) "Cooperative intrusion Tracback and response architecture (CITRA)", IEEE Computer Society Press.
- White, Gregory B. (1996) "Cooperating security managers: a peer-based intrusion detection system", IEEE Computer Society.

Zamboni, D. et al. (1998) "An architecture for intrusion detection using autonomus agents", COAST Laboratory.

## **7.5 Aplicação de Inteligência Computacional (Lógica Fuzzy e Redes Neurais) na Gerência de Redes através da Automatização do uso de Agentes Móveis**

### **7.5.1. Introdução**

Existe uma grande frente de pesquisa na área de agentes móveis aplicado à gerência de redes de computadores que versa em comparar e avaliar as configurações de agentes móveis entre si e com relação a outros paradigmas. Essas comparações e avaliações podem justificar a utilização dos agentes móveis em detrimento de outras opções, tais como a abordagem cliente-servidor.

Existem vários estudos comparando o comportamento de agentes móveis com SNMP [Stallings 1998]. O trabalho de [Rubinstein 2001] faz comparações com SNMP em cima de implementações e modelos aproximados. Existem trabalhos como os de [Arantes 2002], que propõe modelos matemáticos para cálculos de tempo gasto em gerências, por agentes móveis e SNMP, em cima de estudos de casos. Nestes trabalhos percebemos a dificuldade em conceber modelos de avaliação genéricos, pois as implementações de *frameworks* não seguem nenhum padrão. Existem propostas em [Fipa] que sugerem padrões de comunicação entre comunidades e agentes, e que estão disponíveis em documentos como o XC00082B (FIPA Network Management and Provisioning Specification), que especifica padrões utilizados no provisionamento de recursos e na gerência de redes, utilizando agentes ou o XC00084D (FIPA Agent Message Transport Protocol for HTTP Specification) que discorre sobre o transporte de mensagens entre agentes usando HTTP. Esses padrões, apesar de estarem se tornando referência, ainda são utilizados por poucos frameworks disponíveis.

Temos estudos, como [Xavier 2002], que trabalham a comparação entre as várias configurações de comunidades de agentes móveis que uma gerência pode ter. Este trabalho mostra que todas as configurações alcançam os seus objetivos, mas cada uma com características diferentes de obtenção desse objetivo. Mostra ainda que essas diferenças podem ser avaliadas, ajudando na opção por uma configuração mais adequada. Esse trabalho é implementado em cima de um framework de agentes móveis, o KDEMA. Podemos utilizar inteligência computacional no apoio a decisão. Pesquisas que utilizam inteligência computacional em agentes móveis também podem ser encontrados, como em [Karnouskos 2002], onde uma combinação neuro-fuzzy é utilizada para propor um sistema de mensagens inteligente e dinâmico, adaptável às condições do usuário. Em [Das 2002] temos inteligência computacional atuando na distribuição de tarefas a agentes móveis para resolução de pesquisas complexas em bases distribuídas. As métricas analisadas foram tempo e tamanho das pesquisas. Ele apresenta três configurações de pesquisa: um agente, múltiplos agentes ou pesquisa convencional, e sem agentes. Percebemos que o trabalho precisa implementar as configurações para obter decisões, ou seja, não consegue antecipar sobre a decisão mais adequada em tempo de projeto.

Neste trabalho, aplicamos a inteligência computacional na gerência de redes de computadores como uma ferramenta de auxílio ao gerente humano na sua escolha da melhor configuração de agentes móveis. Abordaremos: as relações entre as configurações de agentes móveis e o gerente humano; os modelos matemáticos das configurações; a validação dos modelos matemáticos propostos; a implementação dos modelos matemáticos no KDEMA; o comportamentos das configurações; e como proceder para escolher a configuração de agentes mais adequada com lógica *fuzzy* e/ou redes neurais.

### **7.5.2 Trabalhos em Andamento e futuros**

As configurações propostas não são aleatórias: elas são primitivas sob as quais podemos montar configurações mais complexas, podendo assim adaptar os resultados a ambientes de grande escala (escala aqui se refere também à quantidade de sub-redes a serem gerenciadas, e não somente à quantidade de NEs).

As equações para cálculo do consumo de bytes foram definidas em função de variáveis que as tornam genéricas. Elas admitem quaisquer quantidades de NEs, de instruções da tarefa ou de dados coletados. Após avaliação das configurações, através do modelo de equações, seguida pela implementação no KDEMA, percebemos que essas equações correspondem, com baixa taxa de erro, ao comportamento prático obtido pela implementação.

Definimos um universo de NEs, sob os quais submetemos às equações, encontrando valores de consumo de bytes, que deram origem a gráficos comparativos. Definimos, em seguida, uma função de pertinência, com auxílio de lógica fuzzy, e inferimos os resultados, classificando-os por "muito baixo", "baixo", "médio", "alto" e "muito alto", cada classificação com o seu grau de pertinência (de 0 a 100%).

De posse dessa classificação, oferecemos duas formas de decisão automatizada: por regras de inferência ou por redes neurais.

Percebemos em trabalhos correlatos que existem uma grande dificuldade de avaliar configurações de agentes móveis na prática, dada a falta de padronização entre as implementações. Esses trabalhos adotam como solução, simulações para obtenção de alguns parâmetros, para finalmente avaliar a configuração de agentes.

Contudo, podemos através de modelos matemáticos retirados de um *framework*, obter resultados teóricos bem próximos dos encontrados em suas implementações.

Por outro lado, a gerência de redes de computadores automatizada sempre é desejável, dada a sua possibilidade de pró-atividade e correção de problemas imediatamente após seu surgimento. O modelo de decisão apresentado tenta oferecer ao gerente humano, dadas as suas possíveis atitudes, convertidas em regras de inferência, a decisão de melhor configuração, dada uma gerência.

Não podemos deixar de citar que esse trabalho não contempla gerências condicionais, ou seja, uma coleta de dados, envio de dados ou mobilidade condicionais, os quais equações não podem prever por serem aspectos em tempo de execução.

As equações foram levantadas com características que as tornam genéricas:

- estão divididas em três configurações de comunidades de agentes móveis, dentre as quais uma será eleita a mais adequada;
- estão em função da quantidade de NEs, de forma que podemos aplicar em qualquer quantidade de elementos gerenciados (escalabilidade);
- dada a necessidade de gerência genérica – como por exemplo, a coleta de n dados ou execução remota de determinada rotina, as equações estão também em função das instruções e em função da quantidade de dados coletados;
- definidas em configurações primárias de agentes móveis, ou seja, podemos extrapolar as equações em ambientes complexos, compostos por várias sub-redes, sendo que cada sub-rede teria o seu conjunto de equações, e o resultado para a rede como um todo seria o somatório dos cálculos das partes;

Para uma aplicação dos modelos, podemos então:

- definir a gerência a ser aplicada: coleta de dados, execução remota de rotina;
- implementar as instruções necessárias para tal gerência, através das *Instructions* do KDEMA;
- submeter esses parâmetros ao modelo, obtendo as classificações das configurações;

Nesse ponto já temos ótimos recursos para auxílio à tomada de decisões por parte do gerente humano. Não obstante, podemos ainda nos beneficiar das propostas de tomada automatizada de decisão, da seguinte forma:

- implementação de regras de inferência, de acordo com o contexto e desejos particulares do ambiente-alvo da gerência; vale ressaltar que essas regras serão definidas uma só vez, ou seja, a partir da gerência seguinte, a implementação das regras não seria mais necessária;
- construção de situações de decisão, com entradas e saídas conforme descrito em 7.2, para treinamento de redes neurais; novamente vale ressaltar que essa tarefa seria executada uma só vez;

Esse trabalho nos direciona para as seguintes frentes de pesquisa:

- implementar no KDEMA os recursos de simulação (via equações) das configurações, classificação dos resultados e sugestão de melhor configuração, usando fuzzy e regras de inferência ou redes neurais;
- estudar outros modelos para classificação e escolha de melhor resultado, contemplando gerências condicionais, onde teríamos as equações em função de probabilidades de acontecimentos de gerência;

### 7.5.3 Referências Bibliográficas

[Stallings 1998] Stallings, W. - SNMP and SNMPv2: The infrastructure for network management, IEEE Communications Magazine, 1998.

[Rubinstein 2001] Rubinstein, M. G. (2001) "Evaluation of the performance of mobile agents in the management of networks". Rio de Janeiro.

[Arantes 2002] Arantes, J. A.; Westphall, C.B.; Custódio, R. F. (2002) "Modelo Analítico para Avaliar Plataformas Cliente/Servidor e Agentes Móveis Aplicado à Gerência de Redes". Anais do 20 Simpósio Brasileiro de Redes de Computadores (Vol. I). Búzios (RJ), p. 424-439.

[Fipa] The Foundation for Intelligent Physical Agents, FIPA, <http://www.fipa.org>.

[Xavier 2002] Xavier, E., Koch, F. e Westphall, C.B. (2002) "Avaliação de Variações da Configuração de Agentes Móveis na Gerência de Redes", I2TS'2002 – Florianópolis - SC.

[Karnouskos 2002] Karnouskos, S.; Vasilakos, A (2002) "Neuro-fuzzy applications: Active electronic mail". Proceedings of the 17th symposium on Proceedings of the 2002 ACM Symposium on applied computing.

[Das 2002] Das, S.; Shuster, K.; Wu, C. (2002) "ACQUIRE: agent-based complex query and information retrieval engine". Proceedings of the first international joint conferente on Autonomous agents and multiagents systems.

[Java] Sun Microsystems, 'Java 2 Platform', <http://java.sun.com>.

## 7.6 Arquitetura de *Grids* de Agentes Aplicada à Gerência de Redes

### 7.6.1. Introdução

A computação em *grid* tem surgido como uma iniciativa que possibilita a agregação de recursos conectados em rede, formando um sistema distribuído em larga escala e possibilitando a resolução de problemas científicos e comerciais complexos [Foster 1999]. Distribuindo a carga de trabalho de suas aplicações, um usuário pode dispor de uma capacidade computacional e de armazenamento que se tornariam financeiramente inviáveis de se atingir em um ambiente tradicional.

Este compartilhamento e agregação de recursos se diferenciam das tecnologias atualmente disponíveis na Internet, pela forma como esta integração ocorre. O objetivo é proporcionar um acesso mais barato, eficiente, fácil, abrangente e em larga escala. As diferenças fundamentais entre um *grid* e um sistema distribuído tradicional estão na grande heterogeneidade de recursos, na dinamicidade do ambiente e na alta latência das redes que os interligam. Um *grid* é uma forma de agregação que pode acontecer de várias formas, inclusive através dos mecanismos de cooperação e negociação proporcionados pelos agentes.

No fluxo de trabalho tradicional do gerenciamento de redes temos uma situação onde dados são extraídos dos equipamentos e precisam ser transformados em informações que possam orientar o gerente na tomada de decisões e na execução de ações de gerenciamento [Koch e Westphall 2001]. Sistemas baseados em regras de produção e inferência podem ser utilizados para analisar estes dados, extrair as informações necessárias e identificar possíveis problemas. Porém, a consolidação destes dados em informações de gerência é uma tarefa intensiva e consome um grande poder de processamento. À medida que o ambiente cresce, a eficiência de um sistema centralizado diminui e aumenta o custo com hardware.

Este trabalho apresenta uma arquitetura alternativa, baseada em *grids* de agentes para distribuir a carga destas tarefas intensivas do gerenciamento. Apresentamos os resultados de nossos estudos com *grids* e sua possível aplicação na gerência de redes.

O trabalho abordará: a computação em *grid*, *grids* de agentes e sua utilização na gerência de redes de computadores; nossa proposta para uma arquitetura de *grid* de agentes voltada à gerência de redes de computadores; e nossa arquitetura com outras abordagens.

### 7.6.2 Trabalhos em Andamento e Futuros

Neste trabalho apresentamos uma arquitetura de *grids* de agentes aplicada à gerência de redes de computadores. Também mostramos os conceitos envolvidos com a computação em *grid* e as vantagens de sua utilização no processamento e análise de dados de gerência.

*Grids* de agentes é um assunto relativamente novo e sua utilização na gerência de redes deverá ser cada vez mais explorada, sendo este um trabalho original e inédito na área. Nós destacamos as possibilidades de sua utilização e propomos uma arquitetura de *Grids* de Agentes para Gerência de Redes, validando a mesma teoricamente e via implementação de um protótipo que está em desenvolvimento. Aperfeiçoaremos as atividades até aqui realizadas, dando continuidade aos seguintes trabalhos:

1. Desenvolvimento de melhores protótipos, demonstrando as vantagens da utilização de *grids* de agentes através da realização de mais medições.
2. Evidenciar melhor o ponto em que a utilização de um *grid* de agentes passa a ser mais vantajosa e em que ponto deixa de ser.
3. Realizar estudos sobre o balanceamento de carga no *grid* de processamento. Também procurar meios eficientes de divisão das tarefas de análise. Executar mais medições da capacidade de processamento atingida com um *grid* de processamento e suas vantagens em relação as técnicas tradicionais.
4. Investigar melhor a utilização de agentes móveis na análise de dados e no balanceamento de carga. A mobilidade dos agentes proporciona uma migração das atividades de análise atribuídas a eles, melhorando a utilização dos recursos.
5. Melhorar a eficácia das formas de armazenamento, replicação, indexação e recuperação dos dados de gerência pelos agentes do *grid*.

Mostramos as vantagens de se aplicar *grids* de agentes na gerência de redes, reduzindo custos e proporcionando um processamento e análise mais eficiente através da arquitetura desenvolvida. Ainda existe muito a ser feito e acreditamos que a continuidade e o aperfeiçoamento deste trabalho merecem atenção especial de toda comunidade científica que atua na área, por se tratar de uma abordagem nova e promissora.

### 7.6.3 Referências Bibliográficas

AgentLight, Platform for Lightweight Agents, <http://www.agentlight.org>.

- Buyya, R. (2002) "Economic-based Distributed Resource Management and Scheduling for Grid Computing", PhD Thesis, School of Computer Science and Software Engineering Monash University, Melbourne, Australia.
- CoABS DARPA Project, "Control of Agent Based Systems", <http://coabs.globalinfotek.com/>.
- Distributed.Net Project, <http://www.distributed.net/>.
- Edwards, W. K, Core Jini, Addison Wesley, 1999.
- FIPA SC00001L, "FIPA Abstract Architecture Specification", <http://www.fipa.org/specs/fipa00001/SC00001L.html>, 2002.
- FIPA SC00061G, "FIPA ACL Message Structure Specification", <http://www.fipa.org/specs/fipa00061/SC00061G.html>, 2002.
- FIPA PC00091B, "FIPA Device Ontology Specification", <http://www.fipa.org/specs/fipa00091/PC00091B.html>, 2001.
- FIPA SC00029H, "FIPA Contract Net Interaction Protocol Specification", <http://www.fipa.org/specs/fipa00029/SC00029H.html>, 2002.
- FIPA SC00027H, "FIPA Query Interaction Protocol Specification", <http://www.fipa.org/specs/fipa00027/SC00027H.html>, 2002.
- Foster, I. e Kesselman, C. (1997) "Globus: A Metacomputing Infrastructure Toolkit", Intl J. Supercomputer Applications, 11(2):115-128.
- Foster, I, e Kesselman, C. (1999) "The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann", Morgan-Kaufmann, Orlando, FL.
- Gruber, T. R., (1993) "Toward principles for design of ontologies used for knowledge sharing", Technical Report KSL-93-94, Knowledge Systems Laboratory, Stanford University, August.
- Jeffery, Keith G. (2000) "Knowledge, Information and Data", A briefing to the Office of Science and Technology, UK. <http://itd.clrc.ac.uk/ActivityPublications/239>.
- Kock, F. L., Westphal, C. B., (2001) "Decentralized Network Management using Distributed Artificial Intelligence" Journal of Network and Systems Management. Plenum Publishing Corporation. Meddletown, USA (2001, Vol. 9, No. 4). p. 291-313, December.
- Legion A WorldWide Virtual Computer, <http://legion.virginia.edu/>.
- Manola, F. (1999) "Characterizing Computer-Related Grid Concepts", <http://www.obis.com/agility/tech-reports/9903-grid-report-fm.html>.
- Müller, J. P., (1997) "The Design of Autonomous Agents: A Layered Approach", volume 1177 of Lecture Notes in Artificial Intelligence. Springer-Verlag, Heidelberg.
- Rana, O. F., Moreau, L., (2000) "Issues in Building Agent-Based Computational Grids, UK Multi-Agent Systems" Workshop, Oxford.
- Rana, O. F., Walker D. W., (2000) "The Agent Grid: Agent based resource Integration in Problem Solving Environments", 16th IMACS World Congress on Scientific Computation, Applied Mathematics and Simulation, Lausanne, Switzerland.
- SETI@Home - Search for Extraterrestrial Intelligence, <http://setiathome.ssl.berkeley.edu/>.
- Thompson, C., Odell, J., (1999) "Agent Technology Glossary", <http://www.obis.com/agility/tech-reports/9909-agent-glossary.html>.
- United Devices Inc, <http://www.ud.com/home.htm>.
- XML Extensible Markup Language, <http://www.w3.org/XML/>.
- Wijngaards, N. J. E., Overeinder, B. J., Steen, M. van, Brazier, F. M. T., (2002) "Supporting Internet-Scale Multi-Agent Systems". Em: Data and Knowledge Engineering. June 2002, Volume 41, number 2-3, pp. 229-245, June.

## 7.7 Gerência de Redes em Ambientes WEB, WAP e SMS usando as Tecnologias SNMP, WBEM e CORBA

### 7.7.1. Introdução

Neste trabalho, será analisado um ambiente que tem, em sua essência, recursos da plataforma Windows, pois esta plataforma é dominante [MIL01], mas como em qualquer outro ambiente, existem também recursos de outras plataformas. Essas características são encontradas em algumas instituições que requerem total confiabilidade na rede, pois uma falha pode deixar instituições inteiras inoperantes. Dentro deste contexto, este trabalho propõe uma solução eficiente e inovadora para a gerência de alarmes disparados em reação à falhas ocorridas na rede. É proposta uma aplicação que faz a gerência dos alarmes de uma rede garantindo que as notificações das falhas ocorridas sejam repassadas aos responsáveis de forma rápida e eficaz. A captação destas falhas abrange todas as plataformas da rede, mas possui um enfoque especial na plataforma Windows.

Para atender tais características, foi necessária a utilização de tecnologias como WBEM, SNMP e CORBA e a interação da aplicação com o usuário foi utilizada a WEB e WAP. O WBEM (*Web-Based Enterprise Management*) é uma iniciativa da DMTF (*Distributed Management Task Force*) que objetiva a unificação de mecanismos para descrever e compartilhar informações de gerência, sem definir as regras de implementação, permitindo que a indústria desenvolva soluções de gerência padronizadas e baseadas nas tecnologias WEB emergentes. Desta forma, é possível utilizar diversas tecnologias (como por exemplo CORBA/Java) para estender esta estrutura para um objetivo próprio e até mesmo fazer a integração com o SNMP, que é o protocolo mais popular no que diz respeito a tecnologias de gerenciamento de redes [MAL01].

Fazendo uso das características de implementações baseadas na iniciativa WBEM, juntamente com os já consagrados SNMP e CORBA, através de uma aplicação baseada nos conceitos de engenharia de software foi possível criar uma aplicação completa para gerenciar uma rede, flexível para criação de aplicativos com diversos enfoques.

Com a interface dessa aplicação sendo feita baseada na WEB, é possível gerenciar uma rede a partir de qualquer lugar do mundo onde se tenha uma conexão à Internet. As vantagens de usar esse tipo de interface são várias, indo desde a substituição da linha de comando até a economia em treinamento de pessoas especializadas [MAC01]. Além disso, para proporcionar um melhor acesso a informações gerenciais, a utilização de dispositivos WAP vem crescendo ao longo dos últimos anos devido à demanda existente [STU02]. Este protocolo, mesmo com as dificuldades existentes no ambiente *wireless*, mostra-se bastante útil se bem utilizado, principalmente como forma de apoio a ferramentas de gerência.

Este trabalho abordará: aspectos de gerência de redes juntamente com os protocolos e arquiteturas utilizados; algumas ferramentas existentes no mercado e trabalhos que são realizados nesta área; as tecnologias necessárias para o desenvolvimento do sistema (no caso, a tecnologia *Wireless*, com seu protocolo WAP para desenvolvimento de aplicações e o SMS para envio de mensagens curtas, e a arquitetura de objetos distribuídos como CORBA e DCOM); a implementação; e a validação do mesmo em um ambiente de testes.

### 7.7.2 Trabalhos em Andamento e Futuros

O ambiente a ser gerenciado é formado de equipamentos com várias plataformas, sendo a plataforma Windows dominante. Para obter uma gerência efetiva de um ambiente com estas características, a arquitetura de desenvolvimento precisaria oferecer uma boa integração com as redes Windows e também a possibilidade de integração com outras tecnologias necessárias para a gerência das demais plataformas. Isto se tornou possível com a utilização do conceito de componentes. Alguns componentes foram construídos para o gerenciamento de recursos com a plataforma Windows e outros com a função de disponibilizar ao usuário as informações de forma a unificar as informações de gerência captadas por diferentes tecnologias. Para melhor organizar estes componentes, foram criados os módulos do sistema. Em cada um dos módulos gerentes foram utilizadas tecnologias diferentes como o WMI, SNMP e CORBA. Com essas diferentes tecnologias o ambiente pode ser gerenciado de maneira completa e eficiente. As informações captadas por estes módulos foram unificadas através da base de dados e componentes COM de acesso a mesma. Estes componentes interagem com o usuário através das interfaces WEB e WAP do sistema.

Apesar do bom funcionamento da aplicação, algumas particularidades puderam ser observadas ao comparar módulos gerentes utilizados para recuperar informações relacionadas a falhas no sistema. A escolha do WMI foi fundamental para se ter o resultado esperado do ambiente. O fato de se poder implementar especificamente quais os alarmes a serem gerados, foi importante para a diminuição do número de alarmes gerados. Este fator é essencial para a viabilização da aplicação. Ao contrário do SNMP, que gera *traps* que podem ser simples notificações ou problemas críticos. Para este módulo, foi necessária a criação de filtros, para que o gerenciador recebesse somente *traps* realmente importantes. Já no módulo CORBA não existe este problema, pois os alarmes são gerados pelo ORB *Client* por isso é a responsabilidade deste gerar apenas alarmes importantes. Mas por garantia, existe um filtro pela severidade dos alarmes gerados pelo módulo CORBA.

Outra consideração é o fato do WMI só permitir que sejam recuperadas informações do recurso através do *pooling*. Este fato pode vir a ser um ponto negativo quando a rede está congestionada, mas isso não inviabiliza o bom funcionamento da aplicação. Esta já é uma vantagem dos módulos SNMP e CORBA. No módulo SNMP são recuperadas as *traps* enviadas pelos agentes, sem a necessidade do *pooling*. Assim, uma *trap* é gerada somente quando realmente existe o problema. Da mesma forma funciona o Módulo COM, que tem os ORB *Client*

em cada equipamento, assim que for detectada uma falha, o ORB *Client* envia o alarme para o ORB *Server*, sem utilização excessiva de tráfego na rede.

A criação destes três módulos gerentes proporcionou um gerenciamento bastante completo do ambiente com relação a falhas do sistema. Com a extensão desses módulos é possível a construção de uma ferramenta ainda mais completa, para que além do gerenciamento de falhas, se tome decisões de gerência.

Como sugestões para trabalhos futuros a serem realizados podem ser citados:

1. Ampliação do sistema gerenciador de alarmes para um gerenciador de redes, utilizando as vantagens oferecidas pelo WMI unidas pelo SNMP e CORBA. Essa ampliação pode ser no sentido de permitir tomadas de decisões a partir da WEB e dispositivos WAP. Podendo até ser criado um algoritmo para tomar essas decisões de forma automática para alguns casos.
2. Fazer a união dessas tecnologias diretamente na arquitetura WBEM, através de mapeamentos do modelo CIM com alguma outra tecnologia, por exemplo CORBA onde as informações que foram armazenadas em base de dados pudessem ser acessados através da criação desta aplicação, sem perder as funcionalidades já implementadas do WMI.
3. Criar a aplicação utilizando a extensão do modelo CIM como no item 2 e em seguida fazer a verificação da performance das duas aplicações com objetivo de concluir qual seria a melhor maneira, de se utilizar tais tecnologias.
4. Ampliar a aplicação para servir de auxílio para a construção de SLA (*Service Level Agreement*), onde ao definir as variáveis, poderão ser gerados relatórios específicos para auxiliar neste tipo de contrato.

### 7.7.3 Referências Bibliográficas

- [BOU02] BOUTABA, Raouf.; POLYRAKIS, A Andreas. Projecting advanced enterprise network and service management to active networks. *IEEE Network*. [s.l.]. v. 16, n. 1, p. 28 –33, Jan.-Fev. 2002 .
- [FES99] *FESTOR, O.; FESTOR, P.; YOUSSEF,, Ben N.; ANDREY, Laurent. Integration of WBEM-based management agents in the OSI framework IFIP/IEEE International Symposium on Distributed Management for the Networked Millennium, 1999. Proceedings ...[s.l.]: IEEE Press. 16 p., p 49 – 64.*
- [GAR98] Voth, Gary.R.; Kindel, Charles; Fujioka, Jon. Distributed application development for three-tier architectures: Microsoft on Windows DNA *IEEE Internet Computing*, [s.l.], v. 2 n. 2, Março – Abril 1998 , p. 5, p. 41 –45.
- [GUI01] GUIAGOUSSOU, M.H.; BOUTABA, R.; KADOCH, M. A Java API for advanced faults management. *IEEE/IFIP International Symposium on Integrated Network Management, 2001, Seattle Proceedings...* [s.l.]: IEEE Press, 2001 16 p., p. 483 –498.
- [HON01] HONG, Liu; DONG, Bai; WEI, Ding . The integration of SNMP and web in embedded devices. *International Conferences on Info-tech and Info-net, 2001, Beijing. Proceedings...* [s.l.]: IEEE Press, 2001, 5 p., p. 83 –87.
- [KET02] KETTSCHAU, H.-J.; BRUCK, S.; SHEFCZIK, P. LUCAS - an expert system for intelligent fault management and alarm correlation. *Network Operations and Management Symposium, 2002. Proceedings...*[s.l.]: IEEE Press. 3p., p. 903 –905.
- [MAC01] MACHADO, Christiano.M.;SAFE, Geórgia.P.; NOGUEIRA, José Marcos.S.; LOUREIRO, Antonio A.F. On the impact of using Web interfaces in a distributed management platform. *EEE/IFIP International Symposium on Integrated Network Management, 1, Seattle, 2001. Proceedings...*[s.l.]:IEEE Press. 2001 p. 4, p. 317 – 320.
- [MAL01] MALOWIDZKI, Marek. The management of the mobile network with COM+ and SNMP. *Military Communications Conference,2001, Washington . Proceedings...*[s.l.]: IEEE Press, 2001. 5 p., p. 1456 –1460.
- [MIC99] MICROSOFT, Corporation. *Introducing Windows DNA: Framework for a New Generation of Computing Solutions.* Disponível em: <<http://www.msdn.microsoft.com/library/> > .Acesso em: 25 abril 2002.
- [MIL01] MILANOVIC, Nadza.; MORNAR, Vedran. A software infrastructure for distributed computing based on DCOM. *International Conference on Information Technology Interfaces, 2001, Pula, Croacia . Proceedings...*[s.l.]:IEEE Press, 2001, 6 p., p. 63 – 68.
- [STU02] STUCKMANN, Peter; HOYMANN, Christian. Performance evaluation of WAP-based applications over GPRS. *IEEE International Conference on Communications,2002, New York. Proceedings...* [s.l.]: IEEE Press, 2002, p. 5, p. 3356 –3360.
- [VOU01] VOUGIOUKAS, Stavros; ROUMELIOTIS, Manos. A system for basic-level network fault management based on the GSM short message service (SMS). *International Conference on Trends in Communications, 2001, Bratislava. Proceedings...*[s.l.]:IEEE Press, 2001. 5 p., p. 218 –222, v. 1.

## 7.8 Gerência de Acordos de Níveis de Serviços para Redes Sem Fio

### 7.8.1. Introdução

No momento atual, a crescente competitividade do mercado tem requerido níveis elevados de eficiência e qualidade das organizações. Padrões de qualidade e produtividade nos serviços prestados são fortemente exigidos, como elemento diferencial de sucesso.

Para os provedores de serviços de telecomunicações ou de redes um dos diferenciais em relação aos demais competidores, é a capacidade de executar a Gerência de Nível de Serviço - *SLM*, pela qual o cliente e o provedor podem monitorar a infra-estrutura de comunicação fornecida, garantindo uma maior qualidade, redução dos custos e segurança em suas operações. A gerência de níveis de serviços é definida através de contratos - *SLAs* estabelecidos durante a fase de contratação do serviço, que é utilizado tanto pelo cliente quanto pelo provedor, para verificar os níveis de serviços providos.

As tecnologias baseadas em radio frequência, surgem com bastante força no mercado, como é o caso das redes *ad-hoc*, as quais combinam funcionalidade, flexibilidade, conectividade de dados, mobilidade de usuários em diversos ambientes. Sendo assim, este trabalho tem como objetivo obter através de simulações informações de desempenho nas redes sem fio *ad-hoc* e analisar estas informações a fim de moldar parâmetros de qualidade de serviço, que compõem os *SLAs*, providos sobre estas redes, garantindo assim o seu melhor funcionamento.

Este trabalho aborda: os trabalhos correlatos que levaram o desenvolvimento deste trabalho; a descrição da tecnologia sem fio (*wireless network*), bem como, os principais conceitos, a tecnologia de transmissão sem fio, as técnicas de espalhamento espectral, o provimento de serviços usando redes sem fio, a aplicabilidade e viabilidade destas redes; os parâmetros de QoS utilizados na elaboração e gerenciamento dos acordos de níveis de serviços; e o cenário para o desenvolvimento das simulações.

A gerência de níveis de serviço em redes sem fio poderá ser especificada, modelada e implementada utilizando-se diferentes enfoques e concepções. Na pesquisa desenvolvida, considerou-se referencial existente nos diferentes segmentos interessados por *SLM*, *SLA* e *Redes Sem Fio*. Dentre estes segmentos destacam-se organismos de padronização e fóruns (OMG, ITU-T, ISO, TMForum, IETF, DMTF, IEEE), produtos, serviços, provedores de serviços, fabricantes de *hardware* e *software* e pesquisas da comunidade acadêmica.

Dentre estes segmentos, considerados de extrema relevância para a gerência de *SLM/SLA*, estão os trabalhos desenvolvidos pelo TMForum. Desde 1988, o TM Fórum vem produzindo um conjunto de documentos destinados a alcançar, uma interação com o OSS - *Operational Support System* do TMN da ITU-T, mediante o desenvolvimento de especificações necessárias para a construção de sistemas de gerenciamento [STU00].

Além do referencial existente no TMForum, foram considerados os esforços específicos de outros organismos de padronização, cujas especificações relacionam-se com as categorias de conhecimentos abordadas neste trabalho. Dentre as referências consideradas, destacam-se as seguintes fontes de documentação *on-line*: [ITU02, IEEE02, OMG02, ISO02, DMTF02, QoS02].

O TMF 701 produziu um estudo que trata do suporte a garantias formais de satisfação de níveis de serviço, onde foram levantados diversos aspectos para representação da eficiência do provedor e dos seus serviços em termos gerais, os quais são capazes de representar uma ampla variedade de serviços e provedores. O cliente passou a contar, a partir deste estudo, com um mecanismo de verificação e comparação de comunicação entre os diversos provedores. Neste estudo também são identificados quais os parâmetros mais importantes na provisão de QoS.

Os eventos internacionais mais significativos em gerência de redes são o IFIP/IEEE IM – *International Symposium on Integrated Network Management* e o IEEE/IFIP NOMS – *Network Operation and Management*. Nesses eventos, assim como em outros destinados à divulgação de trabalhos na área de gerência de redes (LANOMS - *Latin American Network Operations and Management Symposium*, DSOM - *Workshop on Distributed Systems: Operations & Management* e APNOMS - *Asia-Pacific Network and Management Symposium*) e em publicações como o *Journal of Network and System Management*, os temas *Service Level Management* e *Redes Sem Fio (Wireless)* têm sido pauta constantes. Entre os trabalhos mais relevantes no âmbito deste assunto destacam-se: [PUK00], [LEE02], [PRI01], [SUK02], [IWA00], [HOL00], [RAN02].

Nos eventos nacionais, sendo o de maior expressão o SBRC – Simpósio Brasileiro de Redes de Computadores, encontram-se referências como: [ROC01], [RUB01], [VIE02].

Alguns outros trabalhos como [HOR02], também foram de extrema relevância para elaboração deste trabalho. Este simula um tráfego no *gateway* de uma *scatternet* em uma rede *Bluetooth* com diferentes tamanhos de pacotes, comparando o desempenho dos esquemas de filas *FIFO* com *Stochastic Fair Queuing – SFQ*, *Fair Queuing – FQ* e *Déficit Round Robin-DRR*. Em [CHO99, PAT02] são apresentadas formas de adaptação de banda para redes sem fio *ad-hoc*. Em [LIM02], é proposto a implementação e validação de um mecanismo sobre o princípio de gerência de largura de banda para manter QoS adaptável aplicados as redes sem fio de topologia

*ad-hoc*. Em [RIB02] é apresentado à avaliação do comportamento de um enlace sem fio em ambiente aberto segundo o padrão 802.11b.

### 7.8.2 Trabalhos em Andamento e Futuros

O padrão 802.11 constitui-se em um dos mais complexos da família IEEE 802, por necessitar atender as peculiaridades inerentes ao meio de transmissão.

As redes sem fio *ad-hoc* são a principal tendência dentro da computação móvel e tem diversas aplicações, fundamentalmente em situações onde não existe uma infra-estrutura de rede fixa ou a sua implementação não é viável.

Em um mercado competitivo como a área de telecomunicações, os provedores de serviço precisam cada vez mais satisfazer seus clientes, oferecendo serviços com alta qualidade, sem interrupções, com preços competitivos e com diferenciais que sejam capazes de manter seus clientes atuais satisfeitos, além de conquistar novos clientes. Um destes diferenciais tem sido justamente a gerência de nível de serviço onde o cliente é capaz de verificar a infra-estrutura de comunicação fornecida verificando possíveis violações no contrato com o provedor de serviços.

Neste trabalho, realizou-se uma análise dos aspectos e dos critérios necessários para elaboração de um SLA, discutindo-se as principais necessidades para implementação de um projeto de SLA em redes *wireless*. Realizou-se também uma avaliação da importância e dos benefícios da implementação do SLA em redes de telecomunicações como melhoria da eficiência e controle de qualidade. Coletaram-se os valores correspondentes a diferentes métricas para analisar como está se comportando o tráfego, assim como os possíveis erros e problemas que podem estar acontecendo no ambiente *ad-hoc* simulado.

Através da análise das simulações, verificou-se que a variação do tamanho do pacote e a taxa de retransmissão influenciam diretamente na latência, na taxa de perdas, no *jitter* e na vazão. Sendo assim, estes parâmetros são condições totalmente dependentes da situação da fila em cada momento. Não somente em termos de pacotes enfileirados, mas também dos perfis destes pacotes, ou seja, se maiores ou menores.

A vazão alcançada ao longo de um ambiente *ad-hoc*, se dá em função do tamanho deste ambiente. Uma rede com apenas dois nodos, alcança uma vazão aproximada, de 1,7 Mbps, para um pacote de tamanho igual a 1500 bytes, e 1,3 Mbps, para um pacote de tamanho igual a 550 bytes, ao invés de 2 Mbps (isso em um rede com canal de 2Mbps), devido ao *overhead* dos cabeçalhos, RTS, CTS e pacotes ACK. A vazão para redes com 30, 40 e 50 nodos mantem-se praticamente a mesma.

Verificou-se a possibilidade de aprofundar os estudos e experimentos realizados no âmbito das redes sem fio. Além dos quatro parâmetros básicos de QoS abordados neste trabalho, outros fatores de QoS que advem da mobilidade e de sua imprevisibilidade se tornam importantes.

Em [SUK01, PAT02, TIA98] a probabilidade de cancelamento devido ao *handoff* é usada como parâmetro de QoS. Este parâmetro é definido como a probabilidade de que a chamada seja cancelada durante o *handoff* devido ao fato da nova célula não possuir recursos suficientes para suportar a chamada. Em [SEA96], os autores identificam um novo parâmetro de QoS para ambientes móveis denominado *loss profile*. Este parâmetro pode ser usado por aplicações que toleram perda. O *loss profile* é definido como uma descrição, provida pela aplicação, da maneira aceitável na qual dados podem ser descartados no caso de redução de largura de banda na parte correspondente ao enlace sem fio. Este parâmetro especifica a taxa de perda aceitável e o comportamento da perda. Em [PAT02], a probabilidade de comunicação transparente (*probability of seamless communication*) é introduzida. Este parâmetro reflete os níveis aceitáveis de interrupção em um serviço devido ao movimento entre células. Aplicações que não podem tolerar qualquer interrupção no serviço devem requisitar uma alta probabilidade enquanto outras aplicações podem requisitar uma probabilidade mais baixa.

Além dos parâmetros mencionados acima, *handoff*, *loss profile* e probabilidade de comunicação transparente, destacam-se ainda: Conectividade, Nível de Ruído (Qualidade do Sinal) e Perda ou Ganho do Sinal.

### 7.8.3 Referências Bibliográficas

- [CHO99] CHOI, S. Qos Guarantees in Wireless/Mobile Networks. Dissertação para o grau de Doctor of Philosophy. University of Michigan, 1999.
- [DMTF02] DMTF, The Distributed Management Task Force. <http://www.dmtf.org>. Acesso em Setembro de 2002.
- [HOL00] HOLLAND, G.; VAIDYA, N. Analysis of TCP Performance over Mobile Ad Hoc Networks. Texas A&M University. 2000.
- [HOR02] HORSTMANN, G. Avaliação de Esquemas de Fila para o Host Controller Interface do Bluetooth. UFSC, Dissertação de Mestrado, 2002.
- [IEEE02] IEEE – Institution of Electrical and Electronic Engineers. <http://www.ieee.org>. Acesso em Setembro de 2002.

- [ISO02] ISO - International Organization for Standardization. <http://www.iso.org>. Acesso em Setembro de 2002.
- [ITU02] ITU-T - Study Group. <http://www.itu.int/ITU-T>. Acesso em Novembro de 2002.
- [IWA00] IWATA, A.; FUJITA, N. A Hierarchical Multilayer QoS Routing System with Dynamic SLA Management. IEEE Journal On Selected Areas In Communication, Vol. 18, No. 12, December 2000.
- [LEE02] LEE, H.; KIM, M.; Hong, J. Mapping Between QoS Parameters a Network Performance Metrics for SLA Monitoring. APNOMS 2002.
- [LIM02] LIMA, A.; WESTPAHLL, C. A Bandwidth Management Adaptive Mechanism for Ad Hoc Wireless Network. SBRC 2002.
- [MAH00] MAHADEVAN, I.; SIVALINGAM, K. Architecture and Experimental Framework for Supporting QoS in Wireless Networks Using Differentiated Services. ACM/Baltzer Mobile Networks and Applications Journal, May 2000.
- [MIR00] MIRANDA, S.; NOGUEIRA, J.; MACHADO, C. Um Sistema de Suporte ao Gerenciamento do Nível de Serviço – SGSWeb. SBRC 2000.
- [NET02b] Network Computing: Wireless Networks: O padrão IEEE 802.11b para redes sem fio. Disponível em: <http://www.networkdesigners.com.br/Artigos/wireless/wireless.html>. Acesso em Agosto de 2002.
- [OMG02] OMG - Object Management Group. <http://www.omg.org>. Acesso em Setembro de 2002.
- [PAT02] PATI, H.; MALL, R.; SENGUPTA, I. An efficient Bandwidth reservation and call admission control scheme for wireless mobile networks. Elsevier, Computer Communications 2002.
- [PRI01] PRIETO, A.; BRUNNER, M. SLS to DiffServ configuration mappings. DSOM 2001.
- [PUK00] PUKA, D.; PENNA, M.; PRODOCIMO, V. Service Level Management in ATM Networks. The International Conference on Information Technology: Coding and Computing (ITCC'00). IEEE. Las Vegas, Nevada. March 2000.
- [QoS02] QoS Forum, Technology Working Group. <http://www.qosforum.com>. Acesso em Setembro de 2002.
- [RAN02] RANDHAWA, T.; HARDY, R. SNMP based Over-the-Air Management of Multi-Mode Mobile Hosts. 2002.
- [RAY02] RAYES, A. Common Management Architecture For Third Generation Wireless Networks. IEEE 2002.
- [RIB02] RIBAS, J. Perfil de Link Sem Fio em Ambientes Aberto: Avaliação Através de Medições. UFSC. Dissertação de Mestrado, 2002.
- [ROC01] ROCHA, R. Uma Arquitetura para Simulação Flexível de Protocolos para Computação Móvel. USP. Dissertação de Mestrado, 2001.
- [RUB01] RUBINSTEIN, M.; REZENDE, J. Qualidade de Serviço em Redes 802.11. SBRC 2001.
- [SEA96] SEAL, K.; SINGH, S. Loss profiles: A Quality of Service Measure in Mobile Computing. Wireless Networks 1996.
- [STU00] STURN, R.; MORRIS, W.; JANDER, M. Foundations of Service Level Management. Editora Campus, 2001.
- [SUK01] SUK-UN, Y.; LEE, J.; LEE, K.; KANG, C. QoS Support in Mobile/Wireless IP Networks using Differentiated Services and Fast Handoff Method. IEEE 2001.
- [TMF02] TMFórum. <http://www.tmforum.org>. Acesso em Setembro de 2002.
- [VIE02] VIEIRA, E.; WESTPHALL, C.; PEREIRA, M. Uso de Especificações Fuzzy-QoS para Gerenciar Delay e Delay Jitter de Conexões TCP. SBRC 2002.

## 7.9 Qualidade de Serviço (Perdas de pacotes, Latência e *Jitter*) em Redes Sem Fio Ad Hoc

### 7.9.1. Introdução

Os roteadores de redes implementam diferentes esquemas de filas para seleção e bufferização de tráfego. Muitos esquemas têm sido amplamente estudados, analisados e desenvolvidos. Sob a mesma ótica pode ser visto o

dispositivo que recebe o tráfego de uma *piconet* cujo destino é outra *piconet*, ou seja, tráfego de *scatternet*. Entretanto, a bufferização deste tráfego em dispositivos *Bluetooth* é implementada adotando um esquema FIFO, que não oferece nenhuma forma de tratamento de tráfego, o que implica na falta efetiva de qualidade de serviços.

No esquema tradicional FIFO, os pacotes são eliminados quando a fila está congestionada. Mas novos esquemas foram desenvolvidos impactando no desempenho dos sistemas, implementando alternativas para tratamento do tráfego ao realizar a bufferização. Podem ser citados: *Fair Queueing* [Abuamsha e Pekergin 1998], *Stochastic Fair Queueing* [McKenney 1991], *Deficit Round Robin* [Shreedhar e Varghese 1995] além de outros.

Os objetivos e metas deste trabalho são realizar uma comparação entre os esquemas de filas *First In First Out (DropTail)*, em comparação com os esquemas *Fair Queueing*, *Stochastic Fair Queueing* e *Deficit Round Robin*, através da simulação de um canal ACL simétrico com 433 Kbits/seg e sentido unidirecional. Para a simulação foi utilizado o software *Network Simulator 2* [Fall e Varandhan 2001] com o objetivo de obter uma visão ampliada do comportamento dos esquemas de filas; avaliar o enfileiramento na *scatternet* e *piconet*; e avaliar a latência e o *jitter* na *scatternet*. Os resultados apresentados neste artigo são baseados nas simulações de uma *scatternet*, com um *slave* atuando como *gateway*, tráfego unidirecional. Foram tabulados os resultados da *piconet* de origem e o comportamento no *master*. Quando o tráfego está no dispositivo *master* já pode ser considerado como tráfego da *scatternet*, por destiná-lo ao nó *gateway*.

Este trabalho aborda: inicialmente uma introdução ao *Bluetooth*, comentando a estruturação da sua pilha de protocolos e o *host controller interface*; conceitos dos esquemas de filas; e o problema e os resultados das simulações.

### 7.9.2 Trabalhos em Andamento e Futuros

Nas variações simuladas, com dois tamanhos de filas, constatou-se que um aumento de 66% na tolerância do limite, passando de 30 para 50 pacotes, houve uma redução de 20% na perda de pacotes, com um aumento de atendimentos, no mesmo tempo de análise, de nove pontos percentuais. Os números isoladamente pouco podem indicar diante do aumento na capacidade do recurso. Porém, se considerada a diferença entre pacotes perdidos e pacotes atendidos para o mesmo período de análise, a relação de melhora em 131% o seu desempenho absoluto. Para um mesmo período de tempo, obtém-se um aumento na quantidade de pacotes atendidos e uma diminuição na taxa de perdas. Em contrapartida, os tempos de latência aumentam, pelo maior número de pacotes presentes na fila e pelo maior tempo presente na fila. Em termos de FIFO, observa-se que, enquanto os limites não são atingidos, o mecanismo atende perfeitamente os objetivos de tratar a demanda de pacotes. O problema percebido ao se atingir o limite, uma situação de esgotamento de recursos disponíveis, o mecanismo recusa a entrada sem qualquer critério que não seja o limite de pacotes presentes na fila. No nosso modelo, os limites foram estabelecidos em termos de números de pacotes. Uma variação possível seria a adoção de tamanho da fila em número de bytes. Porém, esta situação já descaracteriza o mecanismo do esquema FIFO. Adotar um critério de seleção de pacotes, implica na presença de um sistema de classificação prévia de pacotes, antes de serem liberados para entrada na fila, que compare, em bytes, o tamanho do pacote com o espaço disponível na fila.

Embora um sistema classificador de pacotes possa alterar os indicadores de desempenho associados com mecanismos de filas, esta possibilidade complementa o sistema de forma geral, mas não modifica o esquema de fila em si. Indicadores de latência, *jitter*, perda de pacotes podem ser melhorados, mas o tempo e desempenho do classificador devem ser inseridos nas análises. Isto implica em acrescentar um novo fator para ser contabilizado no processo. Por ser um esquema que não atua diretamente sobre os elementos da fila, a latência e o *jitter* são totalmente dependentes do perfil de tráfego. Quanto mais variável for tráfego, maior será a variação da latência, conseqüentemente do *jitter*. Embora possa parecer que a latência e o *jitter* sejam mais estáveis quando há menor nível de enfileiramento, esta constatação não é suficiente por si somente. Para complementar, é preciso considerar o perfil dos pacotes que estão presentes na fila. Quanto mais variáveis os pacotes, maior a variação da latência e *jitter*. Embora tenha sido simulado o impacto do aumento do tamanho da capacidade da fila, isto não contribui para a resolução do problema de enfileiramento do *buffer* do *Host Controller Interface* do *Bluetooth*. O esquema continua sendo FIFO. Enquanto que no mecanismo FIFO os pacotes são atendidos pela ordem de chegada dos fluxos, no mecanismo SFQ é implementado um esquema de *round-robin* para todos os fluxos de entrada. Desta forma, são atribuídos recursos de forma equilibrada para todos os fluxos de entrada. Pelo fato do esquema FIFO não implementar qualquer política para tratamento do tráfego da rede qualquer fluxos agressivos pode tomar todos os recursos e preencher a fila exclusivamente com seus pacotes.

O mecanismo de *round-robin* faz com que cada fluxo envie um pacote por vez. Isto significa que há uma distribuição equilibrada entre os diferentes tipos de tráfego. Os fluxos mais agressivos terão o mesmo tratamento que os fluxos mais brandos. Os primeiros terão maior probabilidade de perda de pacotes, pois estarão atingindo o limite atribuído pelo mecanismo SFQ, que é a divisão do limite máximo entre a quantidade de fluxos. A diferença entre os dois mecanismos consiste, basicamente, na forma de retirada de pacotes para envio, na atribuição de limites para cada fluxo de entrada, e na política de rejeição de pacotes. Aplicando o esquema SFQ para substituir FIFO no *Host Controller Interface* obtém-se a garantia de atendimento dos diferentes fluxos de tráfego. No

problema exposto, dois tráfegos, um *best effort* e outro com requisitos de QoS, não necessariamente haverá algum privilégio para um dos tráfegos, mas sim a garantia de que ambos estarão sendo atendidos nas mesmas proporções. Ou seja, o *buffer* não ficará congestionado com somente um tipo de tráfego. Como o próprio *Bluetooth* implementa um mecanismo de QoS, o esquema SFQ somente reforça o processo, ao eliminar o ponto falho do esquema FIFO em meio a este processo. Porém, mesmo com o SFQ resolvendo o problema de congestionamento da fila, os tempos de latência e *jitter* tornam-se o ponto fraco deste esquema, como pode ser observado comparando-se os gráficos dos anexos D e E. Nestes gráficos estão demonstrados os impactos sobre os diferentes pacotes comparados com os esquemas de filas simulados.

Em relação ao esquema FQ, nada pode ser afirmado de forma conclusiva entre os dois mecanismos de filas baseando-se nos resultados obtidos por estas simulações. Enquanto que FIFO atende pela sequência de chegada, FQ também o faz; enquanto que a primeira rejeita pacotes quando atinge os limites estabelecidos, o segundo segue o mesmo comportamento. Nada de conclusivo pode ser deduzido desta análise quando comparada com FIFO. Portanto, não pode ser considerado como um mecanismo apropriado para substituir FIFO no *Host Controller Interface*. A análise deste esquema reforça também a afirmação feita por [Yoram 2001], sobre a sua pouca eficiência, razão pela qual é substituído por outros esquemas, como *Start time Fair Queueing*, *Stochastic Fair Queueing (SFQ)*, *Self-clocked Fair Queueing*, *Eligible Start time Fair Queueing*, *Smallest Eligible Fair Finishing Time First*, baseados em parâmetros com baixo compartilhamento de reservas [Abuamsha e Pekergin 1998]. Com base na figura A5, observa-se que o mecanismo DRR tem o melhor desempenho se comparada com FIFO. E com o suporte dos gráficos da latência e *jitter* por pacotes, pode-se afirmar que esta é a melhor alternativa para solucionar o problema apresentado. Se a fila do *Host Controller* pode ficar congestionada com um tipo de tráfego quando utilizado o esquema FIFO, o mesmo não acontece com o esquema DRR. Este esquema, ao privilegiar os tráfegos menos agressivos, tende a distribuir os recursos de forma mais “justa” entre os diferentes fluxos. Embora o modelo tenha sido exercitado com pacotes muito grandes, esta característica não se aplica para a maioria dos dispositivos *Bluetooth*. O *Bluetooth* visa comunicação fácil e rápida, portanto, pacotes pequenos, mas pode estar sujeito a diferentes fluxos. A interface do *Host Controller* deve privilegiar os fluxos menores, o que pode ser implementado através do esquema DRR.

A continuidade deste trabalho pode ser direcionada para avaliação de outros esquemas. Inclui-se nesta lista esquemas como RED (*Random Early Detection*), WRED (*Weighted Random Early Detection*), e as variações do esquema FQ, *Start time Fair Queueing*, *Self-clocked Fair Queueing*, *Eligible Start time Fair Queueing*, *Smallest Eligible Fair Finishing Time First*. Alguns destes esquemas são utilizados em roteadores, e, se bem observarmos, o dispositivo *Bluetooth* que atua como *gateway* numa *scatternet* pode ser considerado como um roteador. A literatura específica sobre RED é facilmente encontrada em vários sites de pesquisa. Outra oportunidade de trabalho futuro envolve a simulação de tráfego IP sobre *Bluetooth*, com confirmação de recebimento (*round trip*). O simulador ns-2 está configurado para gerar pacotes *TCP Reno*, *NewReno* e *Vegas*. Da oportunidade anterior deriva outra oportunidade de trabalho futuro, e uma das áreas de pesquisa que ainda permanece aberta em relação ao *Bluetooth* e redes *ad hoc*, relacionadas com mecanismos de reserva de banda através do protocolo *Resource Reservation Protocol (RSVP)*. Seguindo na mesma linha, uma abordagem interessante que surgiu durante a realização deste trabalho, é a elaboração de uma proposta de mecanismos de QoS similares ao esquema *Differentiated Services (DiffServ)*. Considerando que alguns nós estejam fixos em determinada área de cobertura, estes nós poderiam implementar características de serviços que habilitem a formação de *scatternets* com qualidade de serviço. Para minimizar as características de imprevisibilidade de movimentos, típicos de redes móveis, as propostas anteriores podem ser complementadas com algoritmos de previsibilidade de tráfego.

### 7.9.3 Referências bibliográficas

- Abuamsha, Oula and Pekergin, Nihal (1998) “Comparison of Fair Queueing Algorithms with a Stochastic Approach”, In: Proceedings of Mascots’98, pages 139-144.
- McKenney, Paul E. (1991) “Stochastic fairness queueing”, In: Internetworking: Research and Experience, Vol. 2, pages 113-131, January.
- Shreedhar, M. and Varghese, G. (1995) “Efficient fair queueing using deficit round robin”, In: Proceedings of ACM SIGCOMM’95, August.
- Fall, K. and Varadhan, K. – editors, (2001) “The ns Manual (formerly ns Notes and Documentation)”, <http://www.wisi.edu.nsman/ns/ns-documentation.html>, The VINT Project, UC Berkeley, LBL, USC/ISI and Xerox Park, work in progress, March 23, 2002.
- Ericsson, “Specification of the Bluetooth System”, v 1.1, <http://www.Bluetooth.com>, February 22, 2001.
- Miller, Michael (2001) “Descobrimos o Bluetooth”, trad. Altair Dias Caldas de Moraes e Claudio Belleza Dias, Rio de Janeiro, Campus.
- Demers, A., Keshav, S. and Shenker, S. (1989) “Analysis and simulation of a fair queueing algorithm”, In: Proceedings of the Sigcomm’89 Symposium on Communications Architectures and Protocols, 19(4):1-12, September.

Keshav, Srinivasan (1991) "On the efficient implementation of fair queueing", In: Internetworking: Research and Experience, Vol. 2, 157-173, September.

Nagle, John (1987) "On packet switching with infinite storage", In: IEEE Transactions on Communications, COM-35(4), April.

Bernet, Yoram (2001) "Networking quality of service and windows operating systems", New Riders Publishing and Microsoft Corporation, USA.

Zee, Martin van der, and Heijenk, Geert (2001) "Quality of service in Bluetooth Networking" – Part I, Doc. No. 10/0362-FCP NB 102 88 Uen, January

## **7.10 Reconhecimento de Padrões através de Redes Bayesianas e Algoritmo Genético Aplicado à Gerência de Segurança**

### **1. Introdução**

Desde sua primeira geração a telefonia móvel vem provocando mudanças no cotidiano das pessoas, de início com os telefones analógicos, passando para a segunda geração com os telefones digitais e chegando a terceira geração marcada pela convergência da Internet. Estas mudanças que vêm acontecendo requerem cada vez mais serviços seguros, que tornem os usuários confiantes quanto a segurança das redes sem fio [NOT 00].

As questões quanto a segurança para evitar intrusões e fraudes na telefonia móvel se apresentam como a pedra fundamental desta terceira geração de sistemas móveis, onde a interação dos telefones sem fio e a Internet, seja através de comércio eletrônico ou de pesquisa, é a principal característica.

Para a fidelização do cliente e para que ele efetivamente utilize os serviços que já estão a sua disposição e os muitos que estão por vir, as empresas devem alcançar um nível ótimo de proteção de seu sistema. Pois o padrão de consumidores cada vez mais exigentes quanto aos produtos e serviços que irão adquirir, levará a sobrevivência às empresas que estiverem preparadas para as necessidades de seus clientes e que volte seus esforços para a segurança das redes sem fio e Internet.

As empresas de telecomunicações vêm acumulando prejuízos devido a dificuldade de detecção e proteção contra as intrusões e fraudes na telefonia móvel. Pesquisadores se mobilizam na busca da solução para tais problemas, e várias propostas estão surgindo, o que leva a necessidade de sistemas que auxiliem a conquista de melhores resultados garantindo que uma eficaz proteção seja encontrada e que assim possa cumprir sua função de salvaguardar às empresas e seus consumidores. Promovendo o ambiente ideal para que a evolução tecnológica siga seu curso.

Neste trabalho, é realizado um método para análise e classificação dos dados referentes às informações contidas nas ligações telefônicas efetuadas por clientes de uma operadora de telefonia celular. O resultado da análise é essencial para a criação de um sistema mais amplo de detecção de fraude. O método é realizado em duas etapas. A primeira consiste na codificação das variáveis com o intuito de obtermos a transformação dos dados quantitativos originais em dados qualitativos. Com isto, pode-se comparar todos os indivíduos entre si, a fim de se avaliar o grau de semelhança que existe entre eles, bem como avaliar o nível de associação existente entre as características observadas. Após a interpretação dos resultados obtidos com a aplicação desta técnica, poderá ser feito um reagrupamento dos clientes que apresentam perfis similares, referente aos hábitos de como efetuam suas ligações telefônicas, isto é, poderão ser identificados por exemplo os indivíduos que realizam muitas ligações locais e de curta e média duração, ou aqueles que utilizam o telefone para efetuar ligações de todos os tipos, tais como chamadas internacionais de curta duração ou chamadas nacionais de longa duração, dentre outros tipos descobertos.

A segunda etapa, consiste na aplicação de um método de classificação automática, que é proposto neste trabalho, baseado em algoritmo genético e independente de qualquer distribuição dos dados que estão sendo considerados. O algoritmo procura por objetos similares formando assim os diversos grupos(cluster). É proposta uma modificação em relação aos AGs clássicos, permitindo o uso de operadores genéticos mais biologicamente inspirados, onde os pais com boas características genéticas são mantidos durante a formação das próximas gerações. Diferentemente de outras implementações de algoritmo que não levam em conta este fato, esta característica garante a geração de indivíduos cada vez mais aptos, proporcionando um melhor agrupamento (clustering) dos objetos.

### **7.10.2 Trabalhos em Andamento e Futuros**

Desenvolver um Sistema Probabilístico Bayesiano, com o uso do software Netica, capaz de classificar grupos de usuários da telefonia móvel celular, de acordo com suas características de utilização do serviço.

De acordo com a classificação feita, os usuários pertencerão a grupos que apontam sua forma de utilizar o serviço oferecido. O que pode auxiliar a projetos que pretendem a detecção de fraude, ao serem observados comportamentos que fujam as características habituais de uso dos clientes.

Algoritmo genético é uma excelente técnica tanto para resolver problemas de busca em um espaço de características, como para encontrar soluções ótimas. Inspirando-se nestas importantes características dos AGs,

é desenvolvido neste trabalho um algoritmo de agrupamento baseado em algoritmo genético, utilizado na busca dos valores dos centros dos grupos. Sendo o problema de agrupamento a ser resolvido, o enfoque principal recai na execução do AG visando minimizar a métrica de similaridade fornecida. Uma outra contribuição está relacionada com a implementação do AG, no que diz respeito a formação de novas populações. A representação dos cromossomos através de números reais, permite um mapeamento direto entre os cromossomos encontrados e os centros dos grupo.

Como ainda não dispomos dos dados reais, utilizaremos dados artificiais com a finalidade de demonstrar a validade do AG. Inicialmente, a soma da distância Euclidiana absoluta de cada ponto até o seu respectivo centro do grupo será adotada, depois outras métricas poderão ser testadas para comparar os resultados. Outras propostas tais como a representação binária dos cromossomos também podem ser testadas.

A partir das pesquisas resultantes durante este trabalho, pode-se sugerir que se faça uma modelagem orientada à objetos utilizando por exemplo a linguagem de modelagem denominada UML (Universal Modelling Language) do método proposto, pois teríamos uma rápida visão do funcionamento do sistema. E também sugere-se o emprego de novas técnicas de agrupamento baseado em modelos mistos, tais como neuro-fuzzy ou dataming na busca por associações interessantes no espaço de características, bem como a criação de um sistema com base na probabilidade Bayesiana para pesquisar a localização dos fraudadores. Estas considerações, também são importantes no escopo de se tentar resolver o problema de fraude na telefonia móvel.

### 7.10.3 Referências Bibliográficas

[CAE 02] CAETANO, T. Introdução ao Reconhecimento de Padrões. UFRGS - Instituto de Informática, 2002. <http://www.inf.ufrgs.br/~silvia/ipg>

[CAU 91] CAUDILL, M. Expert Network. Byte. Outubro, 1991. p 108-116.

[GAA 96] GAAG, L. C. Bayesian Belief Networks: Odds and Ends. **The Computer Journal**, v.39, n.2, 1996, p.321.

[MIN 68] MINSKY, M. **Semantic Information Processing**, Cambridge: The MIT Press, 1968.

[NAS 98] NASSAR, S. M.; KOEHLER, C. & PIRES, M. M. S. Uma Abordagem Probabilística para Sistemas Especialistas: Avaliação do Estado Nutricional em Crianças de 0 a 2 anos. In: **III Simpósio Nacional de Informática**, Santa Maria, RS, Brasil, 1998.

[PEA 88] PEARL, J. **Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference**. San Mateo: Morgan Kaufmann, 1988.

[RUB 98] RUBIN, A. D. GEER, D.E. A survey of web security. **IEEE Computer**. [S.l.]. v.1. n.31, p-34-41, 1998.

[SIM 01] SIMÕES, P. W. T. A.; NASSAR S. Sistema de Apoio na Avaliação da Falência de Crescimento Infantil. Florianópolis, 2001.

[STE 81] STEVENSON, W. J. Estatística Aplicada à Administração. **São Paulo: Harper e Row do Brasil, 1981**.

[STE 99] STEWART, K. A. EE 4984 telecommunication networks project 1: Celular telephone fraud, 1999. <http://fiddle.ee.vt.edu/courses/ee4984/proj-95/stewart.html>.

## 7.11 Aplicações de XML para Auxiliar na Gerência de Redes

### 1. Introdução

XML (eXtensible Markup Language) é uma metalinguagem que possibilita a definição de linguagens de marcação personalizadas, permitindo a especificação da sintaxe e a validação de documentos nessa linguagem personalizada, chamada aplicação XML. A abordagem de XML, com clara separação entre os dados, a estrutura e a maneira como serão apresentados tais dados, permite que sejam implementados programas que extraiam dados de documentos XML, transforme-os, unifique-os a outras fontes e disponibilize-os para apresentação em vários formatos distintos.

As características de XML tornam-na uma ferramenta ideal para representar dados, apoiando na definição de um modelo de conteúdo padronizado, em uma plataforma aberta, independente de fabricantes e em uma linguagem neutra [Ju 02].

Focando a gerência de redes, o emprego de XML para definir modelos de informação de gerenciamento e processar informação nas aplicações de gerência vem se tornando atrativo [Lewis 01]. Nesse aspecto, XML e suas tecnologias correlatas apresentam vantagens como [Martin-Flatin 00]:

- melhor integração dos dados gerenciados;
- ligação mais flexível entre o objeto gerenciado e aplicação gerente;
- interoperabilidade entre aplicações de gerenciamento de diferentes fabricantes;
- apresentação das informações gerenciais facilidade e estendida para uma ampla variedade de formatos;
- possibilidade de transformação automática das informações de gerenciamento originais, agregando valor decisório nas novas informações produzidas;
- validação dos dados de gerenciamento automática e centralizada.

Neste trabalho é apresentado um enfoque que adota XML para prover uma representação padronizada de dados de gerência de redes. Tais dados, estruturados em documentos XML, podem ser facilmente processados por facilidades fornecidas pela tecnologia correlata a XML (validadores, parsers e transformações), produzindo novos documentos que podem ser *renderizados* em diversos formatos de saída ou servir ainda como entrada para outros sistemas de informação.

### 7.11.2 Trabalhos em Andamento e Futuros

Várias empresas têm questionado os altos custos relacionados às plataformas de gerenciamento. Os fabricantes de equipamentos questionam também o esforço de desenvolvimento para portar suas aplicações de gerência para uma miscelânea de plataformas disponíveis no mercado.

Graças à massificação das redes TCP/IP, a Internet constitui uma infraestrutura ideal para prover intercâmbio de informações. Uma das possibilidades proporcionadas pela *Web* é o acesso e tratamento de informações de gerenciamento de redes. Nessa conjuntura, CORBA já vem sendo utilizada sobre a infraestrutura *Web* como uma ferramenta para permitir a implementação de um sistema de gerenciamento de rede distribuído [Barotto 00] entre as máquinas que compõem a rede, independente de plataforma e com mecanismo de instalação automática, visto que estará disponível através de *browsers Web*.

Apesar da linguagem de marcação HTML ser predominante nos documentos *Web*, suas conhecidas limitações vêm se evidenciando, levando alguns a considerar um momento de colapso para a HTML [Holzner 01]. Tal problemática, somada a grande inserção e aceitação da linguagem HTML como meio de publicação de documentos na *Web*, motivou o W3C a desenvolver a metalinguagem XML [Holzner 01] [Graham 00].

Um esquema padronizado para a portabilidade dos dados pode ser efetivado com a tecnologia XML, que distingue entre interface, processos e dados. Além dessa distinção, XML oferece uma flexibilização no intercâmbio de dados; a possibilidade de personalizar linguagens de marcação, a estruturação, integração e autodescrição de dados. A característica fundamental de XML de dissociação entre estrutura de apresentação e conteúdo do documento, abre espaço para uma revolução na forma como as informações são manipuladas. Um mesmo documento base pode ser automaticamente convertido para diferentes formatos, podendo ser apresentado em um monitor de um computador pessoal, em uma pequena tela de um telefone celular ou até mesmo ser transformado em voz para utilização de deficientes visuais.

Sistemas de gerenciamento de redes que utilizam a *Web* como infra-estrutura de distribuição podem explorar as características de estruturação e flexibilização propiciadas por XML, produzindo documentos de informação de gerenciamento de redes consistentes e formalmente validados. Tais documentos constituem matéria-prima para as mais diferentes aplicações, podendo ser apresentados em inúmeros formatos nos *browsers Web* ou importados por outros sistemas de informação.

### 7.11.3 Referências bibliográficas

- Barotto, André Mello, Souza, Adriano de e Westphall, Carlos Becker. (2000) "Distributed Network Management Using SNMP, Java, WWW and CORBA". *Journal of Network and Systems Management*, v. 8, n.4, p. 251-265.
- Graham, Ian S. (2000) "XHTML 1.0: *Web Development Sourcebook*". New York : John Wiley & Sons.
- Holzner, Steven (2001) "Desvendando XML". Rio de Janeiro: Campus.
- Ju, Hong-Taek; et al. (2002) "An Embedded Web Server Architecture for XML-Based Network Management". *Proceedings of IEEE/IFIP Network Operations And Management Symposium (NOMS)*. Florença, Itália, maio.
- Ju, Hong-Taek, Choi, Mi-Jung e Hong, James W. (2001) "EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management". *Journal of Network and Systems Management*, v. 9, n. 1, p. 31-50.
- Lewis, David e Mouritzsen, Jens D. (2001) "The Role of XML in TMN Evolution". *Proceedings of IEEE/IFIP International Symposium on Integrated Network*, p. 689-702.

- Marchal, Benoît. (2000) "XML By Example". Indianápolis: QUE.
- Martin-Flatin, J. P. (2000) "Web-Based Management of IP Networks and Systems". Ph.D. Thesis, EPFL, Lausanne, Switzerland, outubro.
- McGrath, Sean. (1999) "XML: Aplicações Práticas. Rio de Janeiro". Campus.
- McGrath, Sean. (1998) "Rendering XML Documents Using XSL". Dr. Dobb's Journal, n. 287, p. 82-85, julho.
- Nakhimovsky, Alexander e Myers, Tom. (2000) "Professional Java XML Programming with Servlets and JSP". Birmingham: Wrox Press.
- Stallings, William. (2000) "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3 Ed". Reading, MA: Addison Wesley.
- Ray, Erik T. (2001) "Learning XML: (Guide to) Creating Self-Describing Data". New Jersey: O'Reilly.
- Vlist, Eric Vander. (2001) "XML Schema". New Jersey: O'Reilly.
- World Wide Web Consortium - W3C (2002). "Extensible Markup Language (XML)", <http://www.w3c.org/XML>, maio.

## 7.12 Gerenciamento de Serviços baseados em Políticas sobre Redes de Serviços Diferenciados

### 7.12.1 Introdução

Com os avanços tecnológicos e o uso crescente de redes de computadores, novas tecnologias são necessárias para atender os requisitos pelo aumento de transmissão de dados, processamento de alta performance e qualidade de serviço, estimulando o surgimento de novas tecnologias e o aperfeiçoamento das já existentes. O desenvolvimento de uma tecnologia de transmissão de dados que permita transportar grandes quantidades de dados em altas velocidades a longas distâncias, mantendo principalmente a qualidade de serviço é objeto de pesquisa por parte da comunidade científica internacional.

A tecnologia IP (*Internet Protocol*) atualmente usada na internet, se baseia no melhor esforço (*Best Effort*) faltando funcionalidades para garantir QoS (*Quality of Service*) [15].

A grupos na *Internet Engineering Task Force* – IETF e ATM fórum, que tratam e propõem várias soluções para a QoS na internet. Entre estas se pode destacar o modelo de serviço integrado (*IntServ*) [9], o modelo de serviço diferenciado (*DiffServ*) [10], o *MPLS* [4], engenharia de tráfego [3] e por fim o roteamento baseado em QoS [11].

Todos estes modelos possuem diferentes características, entretanto o principal objetivo é propor soluções de encaminhamento de dados com qualidade e garantias. Ainda nesta linha de pesquisa podemos citar os trabalhos na definição de uma linguagem para a especificação da sintaxe e semântica de políticas de serviços de rede. Onde o gerenciamento baseado em políticas poder orientar o comportamento de um rede ou sistema distribuído completando altos níveis declarativos e redefinindo níveis baixos para otimização geral dos recursos.

Contudo a QoS é um tema de grande relevância e de real aplicabilidade para a comunidade, sendo os resultados de maior importância apresentados em diversos eventos, revistas e jornais da área. A proposta deste trabalho se concentrara no mecanismo de serviços diferenciados, verificando sua principais características em determinadas políticas de gerenciamento de rede e analisando seus resultados.

### 7.12.2 Trabalhos em Andamento e Futuros

O uso de políticas de gerenciamento permite otimizar funcionalidade de recursos, garantir condições para QoS e disciplinar o aproveitamento da largura de banda.

O *NS* possui seis políticas pré-definidas, nas quais qualquer simulação de *DiffServ* terá de usar uma delas.

Os resultados encontrados nas simulações realizadas com estas políticas, refletem as características propostas pelo *DiffServ* como: manipulação rápida dos tráfegos, maior largura de banda na média e menor perda de pacotes.

A idéia deste trabalho é criação de uma política de gerenciamento, para isso a necessidade de incluir módulos dentro do simulador os quais permitam condicionamento, suavização e descarte, dentre outras funções inerentes ao uso deste modelo.

Para tanto, o próximo passo é estudar uma maneira adequada para inserir estes módulos nas classes do *network simulator* e realizar as simulações com as políticas criadas.

### 7.12.3 Referências Bibliográficas

- [1] Trimintzios, P., et al, "A Management and Control Architecture for Providing Differentiated Services in MPLS-Based Networks", IEEE Communications Magazine, Vol. 39, pp 80 - 88, Maio de 2001.
- [2] Agrawal, K., Krishnamoorthy, M., "Resource based Service Provisioning in Differentiated Service Network", IEEE Network, Outubro 2001.

- [3] Xiao, X., Ni., L. M., “*Internet QoS: A Big Picture*”, IEEE Network, Março/Abril 1999.
- [4] T. Li, “*MPLS and the Evolving Internet Architecture*”, IEEE Communications Magazine, Vol. 37, Dezembro de 1999.
- [5] Calvert, Kenneth L., Doar, M. B., & Zegura, E. W., “*Modeling Internet Topology*”, IEEE Communications Magazine, Junho 1997.
- [6] Brunner, M., Quittek, J., “*MPLS Management using Policies*”, IFIP/IEEE International Symposium on Integrated Network Management, 2001.
- [7] Calvert, Kenneth L., Doar, M. B., & Zegura, E. W., “*Modeling Internet Topology*”, IEEE Communications Magazine, Junho 1997.
- [8] VINT Network Simulator, <http://www.masch-cs.berkeley.edu/ns>.
- [9] Braden, R., Clark, D., & Shenker, S., “*Integrated Services in Internet Architecture: An Overview*”, RFC 1633, June 1994.
- [10] Black, D., “*An Architecture for Differentiated Service*”, RFC 2475, December 1998.
- [11] Crawley, E., et al., “*A Framework for QoS-Based Routing in the Internet*”, RFC 2386, August 1998.
- [12] Agrawal, S., Krishnamoorthy, M., “*Resource based Provisioning in Differentiated Service*”, IEEE Network, Abril 2000.
- [13] Surveys. *Lucente Tecnologies*. Disponível em <<http://www.lucentnps.com/knowledge/surveys/00slm>>. Acesso em outubro 2002.
- [14] Sturm, R., Morris, W., Jander, M. – *Service Level Management: Fundamentos do Gerenciamento de Nível de Serviço*, Rio de Janeiro, Campus, 2001.
- [15] Kamienski, C., Sandok, D. et al. *Simulando a Internet: Aplicações na Pesquisa e Ensino*, Sociedade Brasileira de Computação, Florianópolis, 2002.
- [16] Ramanathan, A., Parashar, M., “*Active Resource Management for The Differentiated Services Environment*”, IEEE Communications Magazine, Junho 1999.

## 7.13 Licenças para Distribuição de Conteúdo Online em Sistemas DRM Usando a Linguagem XrML

### 7.13.1 Introdução

Distribuição digital possibilita novos modelos de negócios para o mundo da informação, os quais são muito atrativos para os consumidores, como por exemplo o acesso a áudio digital por serviços de assinatura.

Ironicamente, os serviços de distribuição digital tornaram-se populares devido a sistemas baseados em distribuição ilegal, como o Napster. Este e outros serviços de distribuição ajudaram a mostrar que os consumidores estavam ávidos por novos tipos de serviços e modelos de distribuição de conteúdo digital. Existe uma grande demanda para estes serviços, e os consumidores desejam que o conteúdo seja oferecido numa forma que lhes agrade [Sander 2001].

As novas formas de distribuição de conteúdo por meio da Internet facilitam o comércio de bens e serviços. Porém, questões de segurança e privacidade surgem como desafios para a implantação destes serviços e modelos de negócios. O nível de proteção desejado vai além da simples segurança para a distribuição do conteúdo digital. Questões como a proteção de propriedade intelectual, a confidencialidade de determinados tipos de conteúdos, a privacidade dos usuários ou consumidores, requerem que existam maneiras de fornecer uma “proteção persistente” do conteúdo, ou seja, proteção que permanece com o conteúdo depois deste ser transmitido.

DRM (Digital Rights Management), ou Gerenciamento de Direitos Digitais, pode ser encarado como um termo chave para novos processos de negócios confiáveis, uma tecnologia fundamental para proteger o comércio, a propriedade intelectual, o próprio conteúdo digital, e implementar questões relativas à privacidade.

Uma definição de DRM, segundo [Maclachlan 2001]: “DRM é a corrente de software, serviços e tecnologias que limitam o uso de conteúdo digital ao uso e usuários autorizados e gerenciam quaisquer conseqüências deste uso durante todo o ciclo de vida do conteúdo.”

Em um ambiente empresarial, DRM pode auxiliar no gerenciamento de políticas, as quais controlam o acesso e gerenciamento de informação dentro de uma organização, por exemplo [Duhl and Kevorkian 2001].

Este trabalho aborda: alguns aspectos relevantes sobre o mercado de DRM; a proteção de conteúdo digital através de direitos e licenças; requisitos necessários a uma linguagem de especificação de direitos; e a linguagem específica XrML é apresentada, acompanhada de um exemplo prático de especificação de licença usando esta linguagem.

### 7.13.2 Trabalhos em Andamento e Futuros

A indústria de DRM está atualmente em um processo de consolidação. Grandes empresas estão começando a negociar com conteúdos e serviços que são associados a licenças ou direitos. A mudança das aplicações

centradas em PC para serviços Web é um indicador desta mudança. Além disso, o aumento da conscientização sobre a distribuição digital por entidades legais e a evolução das tecnologias de segurança estão encorajando o comércio de bens digitais.

Grupos como o Oasis Standards Consortium e o IDRM (Internet Digital Rights Management), ligado à IETF (Internet Engineering Task Force), estão discutindo sobre padronizações, regras e aspectos legais, além de outros aspectos relevantes em DRM.

A adoção maciça destes sistemas, como mencionado anteriormente, é uma questão de tempo e experimentação. As tecnologias caminham para soluções como a inclusão de DRM em hardware e em sistemas operacionais, o que auxiliaria na disseminação destas tecnologias.

DRM realiza um papel central neste cenário emergente na Internet. E dentro dos sistemas DRM estão os mecanismos para especificar as informações relativas a direitos e licenças. XrML é um destes mecanismos, e atende às principais exigências deste mercado.

### 7.13.3 Referências Bibliográficas

- Clark, D. (2002) "How Copyright Became Controversial", In: 12<sup>th</sup> Annual Conference on Computers, Freedom and Privacy, USA, April, 10 p.
- ContentGuard, Inc. (2001) "The Need for a Rights Language", Technical White Paper, <http://xrml.org/reference/TheNeedForARightsLanguage.pdf>, USA, 12 p.
- Davis, S. B. (2000) "Beyond Digital Rights – Toward a Digital Media Marketplace", ITGlobalSecure Inc, <http://www.itglobalsecure.com/en/vertical/BeyondDigitalRights.pdf>, USA, October, 10 p.
- Duhl, J. and Kevorkian, S. (2001) "Understanding DRM Systems", IDC White Paper, USA, October, 13 p.
- Erickson, J., Williamson, M., Reynolds, D., Vora, P. and Rodgers, P. (2001) "Principles for Standardization and Interoperability in Web-based Digital Rights Management", In: 2001 W3C Workshop on Digital Rights Management, France, January.
- Feigenbaum, J., Freedman, M.J., Sander, T. and Shostack, A. (2001) "Privacy Engineering for Digital Rights Management Systems", In: 2001 ACM Workshop on Security and Privacy in Digital Rights Management, USA, April, 19 p.
- Fowler, D. (2002) "Digital Rights (and Wrongs)", ACM netWorker, Vol. 6, No. 2, USA, June, p. 26 -30.
- Gunter, C., Weeks, S. and Wright, A. (2001) "Models and Languages for Digital Rights", In: 2001 Hawaii' International Conference in System Sciences, USA, March, 5 p.
- Heileman, G.L. and Pizano, C.E. (2001) "An Overview of Digital Rights Enforcement and MediaRights™ Technology", Technical Report 01-2001, Elisar Software Corporation, USA, April, 21 p.
- Ianella, R. (2001) "Digital Rights Management Architectures", D-Lib Magazine, Vol. 7, no. 6, USA, June, 12 p.
- Ianella, R. (2001) "Open Digital Rights Management", In: 2001 W3C Workshop on Digital Rights Management, France, January, 5 p.
- Intertrust (2001) "About Digital Rights Management", <http://www.intertrust.com/main/overview/drm.html>, USA, November.
- Lam, C.K.M. and Tan, B.C.Y. (2001) "The Internet is Changing the Music Industry", Communications of the ACM, Vol. 44, No. 8, USA, August, p. 62-68.
- Lyon, G. (2001) "The Internet Marketplace and Digital Rights Management", NIST Advanced Technology Program, USA, June, 7 p.
- Maclachlan, M. (2001) "Time Is Coming for Digital Rights Management", <http://www.idc.com/getdoc.jhtml?containerId=ebt20010920>, USA, September.
- Milojicic, D.S., Kalogeraki, V., Lukose, R., Nagaraja, K., Pruyne, J., Richard, B., Rollins, S. and Xu, Z. (2002) "Peer-to-Peer Computing", HP Laboratories Palo Alto, USA, March, 51 p.
- Mulligan, D. and Burstein, A. (2002) "Implementing Copyright Limitations in Rights Expression Languages", In: 2002 ACM Workshop on Digital Rights Management, USA, December, 15 p.
- Park, J., Sandhu, R. and Schifalacqua, J. (2000) "Security Architectures for Controlled Digital Information Dissemination", In: 16<sup>th</sup> Annual Computer Security Application Conference, USA, December, 10 p.
- Röhm, A.W., Herrmann, G. And Pernul, G. (1999) "A Language for Modelling Secure Business Transactions", In: 15<sup>th</sup> Annual Computer Security Applications Conference, USA, December, 10 p.
- Rosenblatt, B., Trippe, B. and Mooney, S. (2002) "Digital Rights Management – Business and Technology", M&T Books, 1<sup>st</sup> Edition, USA, 288 p.
- Sander, T. (2001) "Golden Times for Digital Rights Management?", Intertrust, <http://citeseer.nj.nec.com/489047.html>, USA, November, 12 p.
- Schmelzer, R. (2001) "ContentGuard: XrML – Protecting Digital Resources with XrML", [http://www.xrml.org/Reference/ContentGuard\\_XrML\\_Zapthink.pdf](http://www.xrml.org/Reference/ContentGuard_XrML_Zapthink.pdf), ZapThink, LLC, USA, December, 6 p.
- Stamp, M. (2002) "Digital Rights Management: The Technology Behind The Hype", Technical Paper, USA, August, 16 p.
- Stamp, M. (2002) "Risks of Digital Rights Management", Communications of the ACM, Vol. 45, No. 9, USA, September, p. 120.
- Sun Microsystems (2002) "Digital Rights Management: Managing the Digital Distribution Value Chain", Technical Paper, USA, March, 25 p.

Vora, P., Reynolds, D., Dickinson, I., Erickson, J. and Banks, D. (2001) "Privacy and Digital Rights Management", In: 2001 W3C Workshop on Digital Rights Management, France, January.  
XrML (2002) "eXtensible rights Markup Language", <http://www.xrml.org>, USA, October.

## 8. CONTRAPARTIDA DA INSTITUIÇÃO

O Laboratório de Redes e Gerência (LRG), composto por professores e pesquisadores lotados no Departamento de Informática e de Estatística e também associado ao Curso de Pós-Graduação em Ciência da Computação do Centro Tecnológico da UFSC, apresenta os seguintes equipamentos e recursos para auxiliar no desenvolvimento do Projeto TAGERE – Tópicos Avançados em Gerência de Redes de Computadores e Telecomunicações:

- 1 – Armário de aço – marca Pandim, mod. 402, cor cinza, com 2 portas, com fechadura Méd. 91x41x199cm.
- 8 – Mesas para microcomputador – com tampo em ARVOPLAC, cor branca, com estrutura de ferro, Méd 87x72x74cm.
- 1 – Mesa impressora – com tampo em ARVOPLAC, cor branca, com estrutura de ferro.
- 6 – Cadeiras estofadas, cor preta, com braços laterais.
- 2 – Cadeiras estofadas, cor preta.
- 7 – Cadeiras na cor preta.
- 4 – Transformadores/estabilizadores - marca Power System, mod P515T, 1500 W, alimentação 110/220V, 4 saídas 110V.
- 1 - Mesa para reuniões e trabalho (cor marfim);
- 1 – No-Break – marca Equisul, série Thunder.
- 1 – Impressora jato de tinta – marca HP, Modelo Deskjet-660.
- 1 – Impressora laser – marca HP, modelo LaserJet-4 Plus.
- 1 – CPU/Computador HP Vectra XE 320, Pentium IV, 1.6GHz, 128MB de memória RAM, disco rígido de 40GB, monitor HP modelo D8904 – 60302, teclado e mouse HP.
- 2 – CPU/Computador VTC Samurai Series, 16 MB de memória RAM, disco rígido SCSI 1GB, teclado e mouse.
- 1 - CPU/Computador VTC Samurai Series, 48 MB de memória RAM, disco rígido 1.6GB, teclado e mouse.
- 1 – CPU/Computador Pentium II 300 MHz, 64MB de memória RAM, disco rígido de 4.3GB, teclado e mouse.
- 1 – CPU/Computador Pentium 233 MHz, 64MB de memória RAM, disco rígido de 1.2GB, teclado e mouse.
- 1 – CPU/Computador Pentium III 800 MHz, 192MB de memória RAM, disco rígido de 20GB, monitor Philips 14", modelo 105S, teclado e mouse.
- 1 – Estação SUN – modelo SPARCStation 20, monitor SUN modelo GDM 17E10.
- 1 – Drive SCSI – marca SUN, modelo 6WV411-D, tipo X567-ST, SCSI 2, 2.1 GB.
- 1 – Monitor 14" – marca Deico Electronics, modelo CM-21428
- 1 – Monitor VTC 17" – modelo V5160.
- 2 – Monitor VTC 17" – modelo V5167-UVSYNC 7.
- 1 – Monitor Proview 14" – modelo PV-850D.
- 1 – Monitor TCE 14" – modelo DX460.
- 1 – HUB ACCTRON 10Mbps, 16 portas, modelo EtherHUB- 16mi
- 1 – HUB ADDTRON 10Mbps, 12 portas.
- 3 – Pares de caixas de som para computador.
- 1 – Ar condicionado – marca Cônsul, modelo Air Master, 10000 BTUs.
- 1 - Note Book Magitronic (pentium 166)
- 1 - Televisor Sharp
- 1 - Video cassete Sharp
- 1 - Arcondicionado Electrolux de 7500 BTUs
- 1 - Um tela para projeção
- 2 - Mesas de escritório.
- 1 - Zip Driver Iomega

Além disso, o laboratório conta com livros de gerência, anais de congressos nacionais e internacionais, relatórios de pesquisa, revistas da área de gerência e telecomunicações (da IEEE *Communications Society*, por exemplo). O LRG possui ainda um grupo de alunos de graduação e pós-graduação que poderão atuar como colaboradores do projeto. Complementando, como contrapartida da instituição para realização do projeto a UFSC contribuirá para formação de recursos humanos disponibilizando temas de trabalho em pesquisa para seus alunos de graduação e pós-graduação. Estes alunos também contribuirão bastante para realização do projeto.

## 9. ORÇAMENTO

Segue abaixo o orçamento detalhado sobre custeio e capital que deverão ser alocados pelo Projeto em questão.

PRIMEIRO ANO – MOEDA NACIONAL				
TIPO	DESCRIÇÃO	CÓD.	MATERIAL	VALOR
CUSTEIO	Material de consumo	01	Papel	R\$ 800
			Tonner	R\$ 700
			Cartucho para jato de tinta (preto e colorido)	R\$ 500
			Disquetes	R\$ 400
			Material de escritório	R\$ 200
			Fotocópias	R\$ 500
			Transparências	R\$ 500
			SOMA	R\$ 3 600
	Passagem aérea nacional	03	Três (03) passagens	R\$ 2.000
	Diárias no país	07	Dez diárias no país	R\$ 500
Remuneração de serviços pessoais	09	Serviços de manutenção de equipamentos	R\$ 500	
Outros serviços e encargos	10	Digitações e revisões	R\$ 500	
<b>CUSTEIO</b>			<b>SUBTOTAL</b>	<b>R\$ 7 100</b>
CAPITAL	Equipamentos e material permanente	12	Microcomputador	R\$ 4.000
			Laptop	R\$ 4.000
	SOMA	R\$ 8 000		
	Material bibliográfico	14	Livros e periódicos	R\$ 500
<b>CAPITAL</b>			<b>SUBTOTAL</b>	<b>R\$ 8 500</b>
<b>MOEDA NACIONAL TOTAL</b>				<b>R\$ 15 600</b>

PRIMEIRO ANO - MOEDA INTERNACIONAL				
CUSTEIO	Passagens aéreas	05	Duas (02) passagens	US\$ 4 000
<b>CUSTEIO</b>			<b>SUBTOTAL</b>	<b>US\$ 4 000</b>
CAPITAL	Equipamentos e material	12	Estação de trabalho	US\$ 5 000
			Software de simulação (COMNET III)	US\$ 1 500
			Linguagem de simulação orientada-a-objetos (SIMSCRIPT)	US\$ 1 000
	SOMA	US\$ 9 500		
	Material bibliográfico	14	Assinatura de um journal	US\$ 200
			Assinatura de revistas internacionais	US\$ 400
Livros de Redes e Gerência			US\$ 1 000	
SOMA	US\$ 2 000			
<b>CAPITAL</b>			<b>SUBTOTAL</b>	<b>US\$ 11 500</b>
<b>MOEDA INTERNACIONAL TOTAL</b>				<b>US\$ 15 500</b>
<b>TOTAL PRIMEIRO ANO NACIONAL + INTERNACIONAL</b>				<b>R\$ 69 850</b>

SEGUNDO ANO – MOEDA NACIONAL				
TIPO	DESCRIÇÃO	CÓD.	MATERIAL	VALOR
CUSTEIO	Material de consumo	01	Papel	R\$ 800
			Tonner	R\$ 700
			Cartucho para jato de tinta (preto e colorido)	R\$ 500
			Disquetes	R\$ 400
			Material de escritório	R\$ 200
			Fotocópias	R\$ 500
			Transparências	R\$ 500
			SOMA	R\$ 3 600
	Passagem aérea nacional	03	Três (03) passagens	R\$ 2.000
	Diárias no país	07	Dez diárias no país	R\$ 500
Remuneração de serviços pessoais	09	Serviços de manutenção de equipamentos	R\$ 500	
Outros serviços e encargos	10	Digitações e revisões	R\$ 500	
<b>CUSTEIO</b>			<b>SUBTOTAL</b>	<b>R\$ 7 100</b>
CAPITAL	Equipamentos e material permanente	12	Microcomputador	R\$ 4.000
			Laptop	R\$ 4.000
	SOMA	R\$ 8 000		
	Material bibliográfico	14	Livros e periódicos	R\$ 500
<b>CAPITAL</b>			<b>SUBTOTAL</b>	<b>R\$ 8 500</b>
<b>MOEDA NACIONAL TOTAL</b>				<b>R\$ 15 600</b>

SEGUNDO ANO - MOEDA INTERNACIONAL					
CUSTEIO	Passagens aéreas	05	Duas (02) passagens	US\$ 4 000	
<b>CUSTEIO</b>				<b>SUBTOTAL US\$ 4 000</b>	
CAPITAL	Equipamentos e	12	Estação de trabalho	US\$ 5 000	
			SOMA		US\$ 5 000
	Material bibliográfico	14	Assinatura de um journal	US\$ 200	
			Assinatura de revistas internacionais	US\$ 400	
			Livros de Redes e Gerência	US\$ 1 000	
				SOMA	US\$ 2 000
<b>CAPITAL</b>				<b>SUBTOTAL US\$ 7 000</b>	
				<b>MOEDA INTERNACIONAL TOTAL US\$ 11 000</b>	
				<b>TOTAL SEGUNDO ANO NACIONAL + INTERNACIONAL R\$ 54 100</b>	

TERCEIRO ANO – MOEDA NACIONAL				
TIPO	DESCRIÇÃO	CÓD.	MATERIAL	VALOR
CUSTEIO	Material de consumo	01	Papel	R\$ 800
			Tonner	R\$ 700
			Cartucho para jato de tinta (preto e colorido)	R\$ 500
			Disquetes	R\$ 400
			Material de escritório	R\$ 200
			Cópias xerox	R\$ 500
			Transparências	R\$ 500
	Passagem aérea nacional	03	Três passagens nacionais	R\$ 2 000
	Diárias no país	07	Dez diárias no país	R\$ 500
Remuneração de serviços pessoais	09	Serviços de manutenção de equipamentos	R\$ 500	
Outros serviços e encargos	10	Digitações e revisões	R\$ 500	
<b>CUSTEIO</b>				<b>SUBTOTAL R\$ 7 100</b>
CAPITAL	Material bibliográfico	14	Livros e periódicos	R\$ 500
<b>CAPITAL</b>				<b>SUBTOTAL R\$ 500</b>
				<b>MOEDA NACIONAL TOTAL R\$ 7 600</b>

TERCEIRO ANO - MOEDA INTERNACIONAL				
CUSTEIO	Passagens aéreas	05	Duas passagens	US\$ 4 000
<b>CUSTEIO</b>				<b>SUBTOTAL US\$ 4 000</b>
CAPITAL	Equipamentos e material	12	Assinatura de um journal	US\$ 200
			Assinatura de revistas internacionais	US\$ 400
			Livros de Redes e Gerência	US\$ 400
<b>CAPITAL</b>				<b>SUBTOTAL US\$ 1 000</b>
				<b>MOEDA INTERNACIONAL TOTAL US\$ 5 000</b>
				<b>TOTAL DO TERCEIRO ANO NACIONAL + INTERNACIONAL R\$ 25 100</b>
				<b>TOTAL GERAL DO PROJETO INTEGRADO R\$ 149 050</b>

## 10. AGRADECIMENTOS

A toda equipe do LRG (Laboratório de Redes e Gerência) da UFSC e aos colaboradores nacionais e internacionais pelo auxílio na elaboração do Projeto TAGERE.

## 11. REFERÊNCIAS BIBLIOGRÁFICAS

- BAROTTO, A. M.; SOUZA, A; WESTPHALL, C. B. Distributed Network Management using SNMP, JAVA, WWW and CORBA. Journal of Network and Systems Management. Plenum Publishing Corporation. Meddletown, USA , Vol. 8, No. 4. Pg. 483-497 (Dec. 2000).

- LIMA, Abiel Roche; OLIVEIRA, Sandro Silva; TOKUNO, Douglas Braz; VEZZARO, Rodrigo; WESTPHALL, Carlos Becker. Gerenciamento da Performance do Enlace Sem Fio que faz parte da Internet2 em Santa Catarina. ICIE. Buenos Aires, 23-27 de abril de 2001.
- OLIVEIRA, Sandro Silva; WESTPHALL, Carlos Becker. Qualidade de Serviço na Integração de Redes IP com ATM. ICIE. Buenos Aires, 23-27 de abril de 2001.
- SEKKAKI, A.; ALVAREZ, L. M. C.; WATANABE; W. T.; WESTPHALL, C. B. Development of a Prototype Based on TINA Accounting Management Architecture. IFIP/IEEE International Symposium on Integrated Network Management. Seattle, Washington, USA, 14-18 May 2001.
- MULLER, M. D.; NGUESSAN, D.; WESTPHALL, C. B.; SEKKAKI, A. Um modelo de plataforma de segurança de contabilização na Arquitetura TINA. WTMN - Workshop de Gerência e Serviços de Telecomunicações . Simpósio Brasileiro de Redes de Computadores. Florianópolis, 21-25 de maio de 2001.
- SARI, S. T.; BARROS, A. B.; WESTPHALL, C. B. Measures of Latency on High Performance Processing Environment. Workshop da Rede Nacional de Pesquisa. Simpósio Brasileiro de Redes de Computadores. Florianópolis, 21-25 de maio de 2001.
- KIELING, A. B.; VIEIRA, E. M.; WESTPHALL, C. B. Uma biblioteca de classes para medição de serviços diferenciados. Workshop da Rede Nacional de Pesquisa. Simpósio Brasileiro de Redes de Computadores. Florianópolis, 21-25 de maio de 2001.
- SEKKAKI, A.; NGUESSAN, D.; MULLER, D. M.; WESTPHALL, C. B. Security within TINA Accounting Architecture Management. IEEE International Conference on Communications. Helsinki - Finland. 11-15 June 2001.
- SEKKAKI, A.; ALVAREZ, L. M. C.; WATANABE; W. T.; WESTPHALL, C. B. Accounting Management based Service Environment in a TINA Architecture. IEEE International Conference on Communications. Helsinki - Finland. 11-15 June 2001.
- SEKKAKI, A.; ALVAREZ, L. M. C.; WATANABE; W. T.; WESTPHALL, C. B. Development of Accounting Management based Service Environment in TINA, JAVA and CORBA Architectures. International Conference on Networking. July 9-13, 2001. CREF, Colmar, France.
- OLIVEIRA, S. S.; WESTPHAL, C. B. Comportamento dos parâmetros de qualidade de serviço em um ambiente de rede Redes TCP/IP com ATM. Congresso Brasileiro de Computação. Itajaí (SC), 20-24 de agosto de 2001.
- AZAMBUZA, N.; PEREIRA, F.; LIMA, A. R.; OLIVEIRA, S. S.; WESTPHAL, C. B. Gerência de uma Rede Metropolitana sem Fio. Congresso Brasileiro de Computação. Itajaí (SC), 20-24 de agosto de 2001.
- BLAY, E.; RISO, B. G.; WESTPHAL, C. B. Contribuições para o processo de implementação de Gerenciamento e Administração de Sistemas de Informação em Ambientes Corporativos: a Abordagem Amiga. Congresso Brasileiro de Computação. Itajaí (SC), 20-24 de agosto de 2001.
- ROSSI, L. L.; SOUZA, I. V.; SEKKAKI, A.; WESTPHAL, C. B. Formal Specification and Verification of the Accounting Model of TINA Architecture using LOTOS and ALDEBARAN. Congresso Brasileiro de Computação. Itajaí (SC), 20-24 de agosto de 2001.
- LIMA, A.R.; MECKLENBURGH, P.A.C.K-S.; WESTPHALL, C.B. Proposal and Validation of a Mechanism to Guarantee QoS for Ad-Hoc Wireless Network. 3rd. IEEE International Conference in Mobile and Wireless Communications Network (MWCN' 2001). Recife (PE), Brazil, 14-17 August of 2001.
- VIEIRA, E.; WESTPHALL, C.B. Using Fuzzy Specifications to Manage QoS. Second IEEE Latin American Network Operations and Management Symposium. Belo Horizonte (MG), Brazil, 30 August - 1 September 2001. Pg. 269-280.
- LIMA, A.R.; MECKLENBURGH, P.A.C.K-S.; WESTPHALL, C.B. Um Mecanismo para Garantir QoS em Redes Sem Fio Ad-Hoc. XIX Simpósio Brasileiro de Telecomunicações. Fortaleza (CE), 03-06 de setembro de 2001.
- WATANABE; W. T.; ALVAREZ, L. M. C.; SEKKAKI, A.; WESTPHALL, C.B. Accounting Management based on TINA Service and CORBA Architecture. XIX Simpósio Brasileiro de Telecomunicações. Fortaleza (CE), 03-06 de setembro de 2001.

- MULLER, M. D.; NGUESSAN, D.; WESTPHALL, C. B.; SEKKAKI, A. Um modelo de Arquitetura de Segurança para TINA Aplicada a Contabilidade. XIX Simpósio Brasileiro de Telecomunicações. Fortaleza (CE), 03-06 de setembro de 2001.
- REIS, A.L.A.; WESTPHALL, C.B. Análise do Uso de Agentes Móveis em Adição à Gerência de Redes SNMP. SEMINC - Semana de Informática de Cascavel. Cascavel, 17 a 22 de setembro de 2001.
- LIMA, A.R.; MECKLENBURGH, P.A.C.K-S.; WESTPHALL, C.B. Um Mecanismo para Garantir QoS em Redes Sem Fio Ad-Hoc. XXVII Conferencia Latinoamericana de Informática - CLEI2001 - Ciudad de Mérida, Venezuela, del 24 al 28 de Septiembre del 2001.
- VARGAS, A.C.A.; SILVEIRA, F.E.; EDWARDS, M.L.S.; WESTPHALL, C.B. Security Management for Intrusion Detection in Telecommunications using Neural Networks. The Fifth Asia-Pacific Network Operations and Management Symposium (APNOMS2001). Sydney, Australia, Sept.26-28, 2001.
- MATOS, A.V.; WESTPHALL, C. B. Gerência de Segurança Utilizando SNMPv3. Anais da 5ª Semana Científica de Informática da UNIRONDON. Cuiabá (MT), 19 de outubro de 2001.
- ALVAREZ, L. M. C.; WATANABE; W. T.; SEKKAKI, A.; WESTPHALL, C.B. Development of a prototype based on TINA. XXI International Conference of the Chilean Society of Computer Science. SCCC 2001, IEEE CS Press. Pg. 50-57. Punta Arenas, Chile, 5-9 November, 2001.
- KOCH, F. L.; WESTPHALL, C. B. Decentralized Network Management using Distributed Artificial Intelligence. Journal of Network and Systems Management. Plenum Publishing Corporation. Meddletown, USA (2001, Vol. 9, No. 4). Pg. 375-388 , Dec. 2001.
- SEKKAKI, A.; SOUZA, I. V.; WESTPHAL, C. B. ROSSI, L. L.; A Formal Specification and Verification of TINA Architecture Service with the Accounting Management Module. GRES 2001 - Colloque Francophone sur la Gestion de Réseaux et Service. Marrakech - Maroc du 16 au 23 Décembre 2001.
- SEKKAKI, A.; ALVAREZ, L.M.C.; WATANABE, W.T.; WESTPHALL, C.B. Development of accounting management based service environment in TINA, JAVA and CORBA architectures. Lecture Notes in Computer Science. ISSN 0302-9743. Springer-Verlag Berlin, Berlin. 2094: 438-448. 2001.
- AIDAROUS, Salah; WESTPHALL, Carlos and SILVEIRA, Fernanda. IEEE Communications Society Committee on Network Operations and Management (CNOM). IEEE Communications Magazine. Vol. 40, No. 1. Pg. 25. January 2002.
- LIMA A. R.; FUNDORA, R. E. M.; WESTPHALL, C. B.; MECKLENBURGH, P.A.C.K-S.G. Quality of Service in Ad Hoc Wireless Networks. VIII Congreso de Nuevas Tecnologías de la Industri de las Telecomunicaciones y la Electrónica. Habana, del 20-22 de Febrero del 2002.
- WESTPHALL, C.M.; FRAGA, J.S.; WESTPHALL, C.B.; BIANCHI, S.C.S. Mandatory Security Policies for CORBA Security Model. IFIP/SEC2002 XVII International Conference on Information Security. Pg. 251-262. Cairo, Egypt, May 7-9, 2002.
- WESTPHALL, C. M.; FRAGA, J. S.; WESTPHALL, C. B.; BIANCHINI, S. C. C. Políticas de Segurança Obrigatórias: Bell e Lapadula no CORBAsec. Anais do 20º Simpósio Brasileiro de Redes de Computadores. Vol. I. Pg. 846-861. Búzios (RJ) de 20 a 24 de maio de 2002.
- ARANTES, J. A.; WESTPHALL, C. B.; CUSTÓDIO, R. F. Modelo Analítico para Avaliar Plataformas Cliente/Servidor e Agentes Móveis Aplicado à Gerência de Redes. Anais do 20º Simpósio Brasileiro de Redes de Computadores. Vol. II. Pg. 424-439. Búzios (RJ) de 20 a 24 de maio de 2002.
- RHODEN, G. E.; MELO, E. T. L.; WESTPHALL, C. W. Detecção de Intrusões em Backbones de Redes de Computadores Através da análise de Comportamento com SNMP. Anais do 20º Simpósio Brasileiro de Redes de Computadores. Workshop em Segurança de Sistemas Computacionais. Pg. 9-16. Búzios (RJ) de 20 a 24 de maio de 2002.
- PONTES, K. L.; WESTPHALL, C. M.; WESTPHALL, C. B. Proposta e Implementação de Protocolo de Transferência de Arquivos usando Segurança por Chave Pública (Fast-TP). Anais do 20º Simpósio Brasileiro de Redes de Computadores. Workshop em Segurança de Sistemas Computacionais. Pg. 65-72. Búzios (RJ) de 20 a 24 de maio de 2002.

- FILHO, H. C.; NETO, A. V.; SARI, S. T.; WESTPHALL, C. B. Controle de Acesso às Redes Virtuais Emuladas. Anais do 20º Simpósio Brasileiro de Redes de Computadores. Workshop em Segurança de Sistemas Computacionais. Pg. 65-72. Búzios (RJ) de 20 a 24 de maio de 2002.
- LIMA A. R.; WESTPHALL, C. B.; MECKLENBURGH, P.A.C.K-S.G. A Bandwidth Management Adaptive mechanism for Ad Hoc Wireless Network. Anais do 20º Simpósio Brasileiro de Redes de Computadores. VII Workshop de Gerência de Redes e Serviços de Telecomunicações. Pg. 03-10. Búzios (RJ) de 20 a 24 de maio de 2002.
- PEREIRA, M. C.; VIEIRA, E. M.; WESTPHALL, C. B.; Uso de Especificação Fuzzy-QoS para Gerenciar Delay e Delay Jitter de Conexões TCP. Anais do 20º Simpósio Brasileiro de Redes de Computadores. VII Workshop de Gerência de Redes e Serviços de Telecomunicações. Pg. 73-80. Búzios (RJ) de 20 a 24 de maio de 2002.
- LOBATO, M. R.; KRÜGER, R. T.; WESTPHALL, C. B. Simulação de Redes com o NS2 Anais da II SEPEX (Semana de Ensino, Pesquisa e Extensão) da UFSC. Pg. XX. Florianópolis (SC), 11 a 14 de junho de 2002. (Resumo).
- OLIVEIRA, S.S.; WESTPHALL, C.B. Análise de Tráfego do Protocolo LAN Emulation usando Simulação. II Congresso Brasileiro de Computação. Itajaí (SC), 26-30 de agosto de 2002.
- NAZARENO, D., RISO, B. G., WESTPHALL, C. B. Uma ferramenta para Gerência de Redes ATM, via WWW, Java e SNMP. II Congresso Brasileiro de Computação. Itajaí (SC), 26-30 de agosto de 2002.
- XAVIER, E.; KOCH, F. L.; WESTPHALL, C. B. Avaliação de Variações da Configuração de Agentes Móveis na Gerência de Redes. International Information Technology Symposium. Florianopolis, SC, Brasil October 01-05, 2002.
- ASSUNÇÃO, M. D.; SOBRAL, J. B. M.; WESTPHALL, C. B. Agentes Móveis na Gerência de Redes. International Information Technology Symposium. Florianopolis, SC, Brasil October 01-05, 2002.
- LIMA A. R.; WESTPHALL, C. B.; MECKLENBURGH, P.A.C.K-S.G. Quality of Service fo Ad Hoc Wireless Network. XXII International Conference of the Chilean Society of Computer Science. SCCC 2002, IEEE CS Press. Pg. -. Copiapó, Chile, 4-9 November, 2002.
- GUBERT, L. C. WESTPHALL, C. B. Implementação de uma Ferramenta para Gerenciamento de Tráfego Multicast. VII Jornada de Pesquisa da UNIJUÍ. Ijuí - RS, 04 de novembro de 2002. (Resumo).
- ARMANINI, K. K.; WESTPHALL, C. B.; WESTPHALL, C. M. SeguraWeb: RBAC Framework for Web Applications. GRES 2003 - Colloque Francophone sur la Gestion de Réseaux et Service. Fortaleza (CE), 24 a 27 de fevereiro de 2003.
- ARANTES, J. A.; WESTPHALL, C. B.; CUSTÓDIO, R. F. Client/Server and Mobile Agent Paradigms - An Analytical Model for Performance Evaluation. Colloque Francophone sur la Gestion de Réseaux et Service. Fortaleza (CE), 24 a 27 de fevereiro de 2003.
- REIS, A. A.; WESTPHALL, C. B. Results of experiments with Mobile agents in the execution of network management tasks comparing to SNMP. Colloque Francophone sur la Gestion de Réseaux et Service. Fortaleza (CE), 24 a 27 de fevereiro de 2003.
  - REIS, A. A.; WESTPHALL, C. B. The Use Analysis of Mobile Agents in addition to the SNMP Network management. Colloque Francophone sur la Gestion de Réseaux et Service. Fortaleza (CE), 24 a 27 de fevereiro de 2003.
  - WESTPHALL, C.B.; SEKKAKI, A.; ALVAREZ, L. M. C.; WATANABE; W. T. Prototype Development and Integration between a Security Model and a TINA Accounting Management Architecture. Journal of Network and Systems Management. Plenum Publishing Corporation. Meddletown, USA (2003, Vol. , No. ). Pg. , 2003.
  - WESTPHALL, C. B. Tópicos Avançados em Gerência de Redes de Computadores e Telecomunicações. Livro em edição. Florianópolis (SC), março de 2003. [www.lrg.ufsc.br/hope/livro.pdf](http://www.lrg.ufsc.br/hope/livro.pdf).