Soluções de Gerenciamento Proativo em Redes de Computadores

Mário L. Moura Júnior Antônio A. F. Loureiro Mário F. M. Campos

{mjunior, loureiro, mario}@dcc.ufmg.br

Departamento de Ciência da Computação

Universidade Federal de Minas Gerais

Belo Horizonte - MG

Resumo

Gerenciamento proativo em uma rede de computadores tem como objetivo determinar padrões de comportamentos que indiquem o mais cedo possível cenários indesejados ao bom funcionamento da rede. Esses cenários podem estar associados a configuração, segurança, desempenho, falha e contabilização da rede. Este trabalho discute e compara os principais trabalhos acadêmicos e comerciais relacionados com o gerenciamento proativo e os analisa considerando o contexto das cinco áreas de gerencia de redes.

Abstract

The main goal of Proactive Management in a computer network is to determine behaviors that indicate as soon as possible undesirable scenarios to the proper working of the network. These scenarios may be associated with the configuration, security, performance, fault and accounting in a network. This paper discusses and compares the main proposals from both academia and industry related to proactive management considering the five network management areas.

Palavras chave: Redes de Computadores

1. Introdução

A área de atuação das redes de computadores tem crescido muito nos últimos anos. Em função desse fato e do grande número de fabricantes e protocolos existentes no mercado, o gerenciamento das redes tornou-se uma tarefa complexa porém fundamental no cotidiano das empresas e instituições.

O gerenciamento de redes, quanto ao aspecto comportamental, possui basicamente duas linhas de pensamento [Cruz et al. 1997], não necessariamente excludentes:

- Gerenciamento reativo: Neste tipo de gerenciamento, deve-se esperar a degradação da qualidade dos serviços oferecidos pela rede para a execução de contramedidas. Essa abordagem, apesar de ser adotada na maioria dos *softwares* de gerência disponíveis no mercado, pode contribuir com o aumento do *downtime* da rede em função da incapacidade de se prever possíveis falhas.
- Gerenciamento proativo: Nesta abordagem, é realizado um diagnóstico antecipado e constante da situação da rede de modo que contramedidas possam ser executadas antes que a qualidade dos serviços oferecidos seja degradada. Para implementar um esquema de gerenciamento proativo é necessário fazer um profundo estudo do comportamento dos elementos da rede e da sua topologia de modo a determinar os parâmetros de

operação. [Meira e Nogueira, 1997] apresentam os três passos necessários para a implementação deste tipo de gerência:

a) Classificação dos elementos de rede e de seu comportamento ao longo do tempo.

b) Correlação das informações de toda a rede e formulação de hipóteses.

c) Resolução e verificação para confirmar a verdadeira causa da degradação e solucioná-la.

Este trabalho tem como objetivos discutir e comparar os principais trabalhos acadêmicos e comerciais relacionados com o gerenciamento proativo, analisando-os a partir do contexto das cinco áreas de gerência de redes (configuração, segurança, desempenho, falhas e contabilização).

O trabalho está estruturado da seguinte forma: a seção 2 apresenta conceitos básicos de gerência de redes, gerenciamento proativo e correlação de alarmes. A seção 3 discute implementações de gerência proativa no meio acadêmico. A seção 4 discute algumas implementações comerciais. Finalmente, a seção 5 apresenta as conclusões do trabalho.

2. Conceitos

Nesta seção são apresentados alguns conceitos de gerência de redes e de correlação de alarmes necessários para o melhor entendimento deste trabalho.

2.1 Gerência de redes

A gerência de redes tem por objetivos controlar e monitorar os recursos de *hardware* e *software* em um ambiente computacionalmente distribuído. O controle dos recursos está associado a alteração da configuração dos elementos da rede e suas respectivas conseqüências. A monitoração consiste na observação e análise do *status* e do comportamento dos recursos.

O modelo de referência OSI subdivide a gerência de redes em cinco áreas de conhecimento [Stallings, 1993]:

- Gerência de Configuração: responsável por controlar a configuração da rede de modo a possibilitar sua operação independentemente da existência de recursos com falhas. Deste modo, esta deve ser capaz de manter, adicionar e atualizar as relações entre os diversos recursos.
- Gerência de Contabilização: oferece funções que possibilitam determinar o custo associado à utilização dos recursos.
- Gerência de Desempenho: tem por função monitorar o desempenho dos recursos, alterando (se necessário) as configurações dos que estiverem com desempenho não satisfatório.
- Gerência de Falhas: tem por função fornecer meios que possibilitem a detecção, o isolamento e a correção de falhas na rede.
- Gerência de Segurança: apresenta como função básica restringir o acesso de usuários não autorizados aos recursos de rede.

Uma característica importante a ser levantada é o relacionamento entre as gerências, onde um fato relativo a uma das gerências pode influenciar as demais. Um exemplo de tal situação é a configuração incorreta de um equipamento que pode determinar a ocorrência de falhas e consequentemente a redução do desempenho. Normalmente as gerências de configuração e segurança estão associadas ao controle e as demais ao monitoramento apesar de possivelmente todas estarem relacionadas ao controle e ao monitoramento dos recursos.

2.2 Gerenciamento proativo

O gerenciamento proativo, como dito anteriormente, tem por objetivo realizar um diagnóstico antecipado e constante da situação da rede de modo que contramedidas possam ser executadas antes que a qualidade dos serviços oferecidos seja degradada. Sendo assim, para cada uma das áreas de gerência diferentes abordagens podem ser adotadas. A seguir realizam-se considerações sobre as características desejáveis de aplicações desenvolvidas para cada uma das gerências.

- Gerência de Configuração: uma aplicação de gerência proativa para este cenário deve ser capaz de detectar alterações não autorizadas na configuração dos equipamentos de rede restaurando-as rapidamente aos valores originais, detectar e corrigir configurações incorretas e/ou que não utilizem todo o potencial do recurso em questão, interagir com a gerência de desempenho de modo a otimizar a configuração dos recursos em função do tipo e carga de serviço utilizado, interagir com a gerência de falhas para determinar configurações alternativas no caso de uma emergência.
- Gerência de Contabilização: uma aplicação para este fim pode, em função dos custos e da qualidade de serviço requerida pelo cliente, alocar dinamicamente canais de comunicação, reconfigurar equipamentos e modificar tabelas de rotas. Para isto é fundamental conhecer o padrão de utilização do cliente e suas necessidades.
- Gerência de Desempenho: uma aplicação para este fim deve ser capaz de prever a saturação de um recurso de rede, indicando ao administrador a necessidade de atualização. A aplicação deve ser capaz também de a partir do desempenho geral da rede coordenar alterações na configuração dos equipamentos de modo a otimizar a utilização dos canais de comunicação.
- Gerência de Falhas: uma aplicação para gerência de falhas deve ser capaz de identificar padrões de comportamento que indiquem a possibilidade de ocorrência de falhas. Deste modo, será possível executar contramedidas antes da ocorrência efetiva da falha. Esta aplicação deve também ser capaz de identificar, isolar e corrigir com eficiência falhas que venham efetivamente a ocorrer.
- Gerência de Segurança: aplicações deste tipo devem ser capazes de identificar padrões de tráfego e de consulta a serviços que possivelmente indiquem uma tentativa de acesso não autorizado. Deste modo, será possível rastrear com maior velocidade tais tentativas reduzindo assim as chances de sucesso por parte do invasor.

2.3 Correlação de alarmes

A correlação de alarmes está intimamente ligada ao gerenciamento proativo e consiste em uma das áreas que sofre maior influência desta tecnologia. A correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais. A correlação tem por objetivo reduzir o número de notificações de alarmes, aumentado o conteúdo semântico das notificações resultantes [Meira e Nogueira, 1997].

Um alarme é a notificação de uma ou mais falhas. Uma falha é o nome dado à causa de um mau funcionamento de um recurso da rede. Segundo [Katzela e Shwartz, 1993] o processo de determinação da origem de uma falha é NP-Completo. Com o objetivo de determinar a origem de uma falha em tempo polinomial, foram desenvolvidas várias heurísticas para correlação de alarmes, entre elas o gerenciamento proativo. O leitor interessado pode verificar em [Meira e Nogueira, 1997] uma ampla discussão sobre os métodos desenvolvidos.

3. Gerenciamento proativo no meio acadêmico

Esta seção apresenta diversas implementações existentes no meio acadêmico para o gerenciamento proativo de redes de computadores. A seção 3.1 apresenta uma solução baseada em um sistema especialista para redes locais. A seção 3.2 apresenta um sistema especialista para redes ATM. Na seção 3.3 é descrita uma

implementação baseada em redes bayesianas. Na seção 3.4 é apresentada uma breve discussão sobre as vantagens de um sistema descentralizado. Na seção 3.5 é descrito um algoritmo para correlação de alarmes cujos conceitos envolvidos podem ser aplicados em gerenciamento proativo. Finalmente, na seção 3.6 é realizada uma consolidação dos artigos apresentados nas seções anteriores.

3.1 Rocha e Westphall

[Rocha e Westphall, 1997] apresentam a implementação de uma ferramenta de gerência proativa para o monitoramento de problemas de desempenho e congestionamento na rede local do CESUP – RS (Centro Nacional de Supercomputação). Os autores especificam uma ferramenta que adota técnicas de inteligência artificial com o objetivo de auxiliar a determinação do comportamento dos elementos de rede ao longo do tempo.

A implementação realizada é baseada em um sistema especialista, sendo o desenvolvimento deste tipo de sistema realizado em quatro etapas:

a) Aquisição de conhecimento: A primeira etapa consiste na extração do conhecimento dos responsáveis pelo funcionamento da rede e de especialistas no assunto por "engenheiros de conhecimento". Após o processo de extração, os engenheiros migram as informações para a base de conhecimento sendo esta organizada em conjuntos de heurísticas de modo a obter uma maior eficiência no funcionamento.

b) Estruturação da base de conhecimento: A base de conhecimento apresenta estrutura diferente de um banco de dados convencional pois permite atualizações conforme o contexto. A estrutura da base de dados depende do tipo de conhecimento representado, devendo ser idealmente uma rede semântica com o objetivo de suportar modelagem da estrutura física, *links* causais e relações entre diferentes modelos. Outro fato a ser considerado é que deve ser composta de regras com o objetivo de permitir conhecimento dedutivo.

c) Implementação da máquina de inferência: A máquina de inferência seleciona e aplica a regra apropriada em cada passo do sistema especialista ao manipular a base de dados. A escolha pode ser feita em dois sentidos: ações $\Rightarrow$ objetivo (*forward*) e objetivo $\Rightarrow$ ações (*backward*).

d) Desenvolvimento da interface: A interface deve permitir o monitoramento e a interação do usuário com o sistema.

Segundo os autores, os resultados obtidos foram animadores. Os resultados práticos e teóricos foram apropriados para o gerenciamento da rede e a partir destes foi possível criar um banco de dados com o funcionamento da rede. Como extensão do trabalho, são propostas a adoção de redes neurais para o diagnóstico de problemas e a combinação de técnicas de inteligência artificial e de simulação para incrementar o conhecimento do sistema.

3.2 Cruz et al.

[Cruz et al., 1997] apresentam uma implementação baseada em um sistema especialista para o gerenciamento proativo de desempenho e de falhas em redes ATM. Os autores enumeram os quatro passos necessários para a implementação deste tipo de sistema: aquisição de conhecimento, estruturação da base de conhecimento, implementação da máquina de inferência, desenvolvimento da interface.

Segundo [Cruz et al., 1997], o conhecimento do domínio de um problema deve ser estruturado separadamente dos procedimentos de solução do problema. Ou seja, de um lado, a base de conhecimento armazena o conhecimento especializado, e do outro lado, a máquina de inferência organiza os objetivos e os passos para obtê-los. Esta estruturação é denominada *Sistema Baseado em Conhecimento* e tem como principal vantagem a possibilidade de se utilizar uma mesma máquina de inferência em diferentes bases de conhecimento.

A implementação é baseada no ambiente de desenvolvimento de sistemas especialistas *Kappa*. O *Kappa* é um *shell* cujo funcionamento é baseado em regras de produção e *frames*. A grande vantagem deste ambiente é o fato de possuir uma máquina de inferência já implementada, reduzindo assim, o tempo de desenvolvimento do

sistema. Além disso, por possuir um ambiente próprio de simulação, o processo de aquisição do conhecimento é incrementado.

Os autores concluem o trabalho reafirmando a importância do gerenciamento proativo em uma rede de computadores. Os autores afirmam também que sistemas baseados em raciocínio *forward* são apropriados para simulações e *backward* para diagnósticos.

3.3 Hood e Ji

[Hood e Ji, 1998] apresentam um sistema de gerenciamento proativo para controle de falhas baseado em redes bayesianas. A implementação tem como ponto de partida a adoção de agentes inteligentes capazes de coletar dados SNMP junto aos recursos de rede. Segundo os autores, agentes inteligentes apresentam como principais vantagens: a capacidade de detectar falhas não conhecidas anteriormente correlacionando-as com o tempo e espaço, utilização de poucos recursos de rede, e facilidade de generalização para diferentes tipos de arquiteturas. A adoção do SNMP foi feita em função da sua grande utilização em diversos recursos de rede, facilitando assim, a integração de diferentes plataformas no sistema de gerência.

Redes bayesianas são uma representação gráfica das diversas relações dentro de um domínio de um problema. Para isto é construído um grafo direcionado acíclico (Figura 1), onde os nodos representam variáveis aleatórias e as arestas as relações entre elas. No trabalho, os nodos representam a "saúde" dos elementos de rede, as arestas determinam relações de causa e efeito, e o nodo raiz do grafo representa a saúde de toda a rede. Para se calcular a saúde da rede, os agentes inteligentes calculam a saúde nos nodos folha do grafo a partir dos dados coletados via SNMP e os disponibilizam para os níveis superiores do grafo. Após isto, é realizado um processamento estatístico de todos os resultados disponíveis de modo a definir um valor para a saúde da rede. Um aspecto importante desta abordagem é o fato dos dados de saúde estarem disponíveis também para os nodos folha, por exemplo, se um recurso de rede não estiver operacional, um agente inteligente localizado em um nodo saudável poderia atrasar o envio de uma mensagem até que este se encontre novamente em operação.

Os autores concluem o trabalho definindo o conceito de janela de aprendizado. A janela de aprendizado é o período de referência para o sistema definir os seus limites de operação. Foi verificado experimentalmente que valores entre uma hora e uma semana não tiveram influência significativa nos resultados.

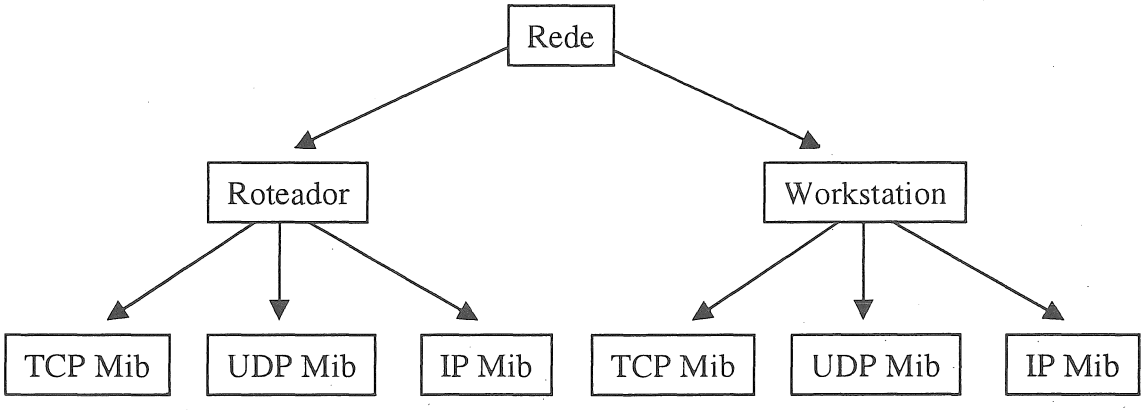

Figura 1 - Exemplo de Rede Bayesiana

3.4 Grimes e Adley

[Grimes e Adley, 1997] apresentam um estudo sobre as desvantagens de um sistema de gerenciamento proativo centralizado e a implementação de um sistema de gerência descentralizado baseado na migração de agentes inteligentes pela rede para controle de desempenho e de falhas.

Segundo [Grimes e Adley, 1997], um sistema de gerência centralizado apresenta como desvantagens:

- Muitas operações são necessárias em situações complexas de teste. Quando um número grande de testes é realizado em conjunto com vários agentes distantes, o gasto de banda é concentrado no gerente, característica não desejável em situações de grave falha.
- Centralização: a inoperância do gerente, seja por falha do mesmo ou do canal que o conecta, implica no imediato cancelamento de todas as ações do sistema de gerência nos nodos folha. Isto ocorre em função da inteligência estar centralizada no gerente e nenhuma ação poder ser tomada sem o seu conhecimento.
- Recursos computacionais: A centralização das ações pode implicar em consumo excessivo de banda, CPU e memória no gerente.

Para evitar este problema, foi proposta uma arquitetura baseada em um agente central mais leve trabalhando cooperativamente com agentes inteligentes espalhados pelos diversos nodos da rede. O agente central envia *scripts* de gerência para os agentes das folhas executarem. Os agentes folha executam os *scripts* e retornam o resultado do processamento para o agente central. A troca de informações entre eles é feita a partir de uma MIB SNMP localizada no cliente. Esta MIB é composta basicamente por três campos:

- Endereço/nome do *script* a ser buscado
- Status da transmissão: sucesso, falha, em progresso
- Resposta do processamento do *script*.

A transferência do *script* para o agente cliente foi feita a partir do protocolo HTTP *(HyperText Transfer Protocol)*. Segundo os autores diversas abordagens foram testadas (FTP, SMTP, HTTP e SNMP), porém o HTTP apresentou implementação mais simples e maior portabilidade para diferentes plataformas.

[Grimes e Adley, 1997] concluem o trabalho afirmando que esta abordagem é mais interessante que a centralizada pois:

- O agente inteligente é dotado de inteligência suficiente para executar o *script* caso a comunicação com o gerente central seja interrompida.
- Os agentes desenvolvidos são menores e consequentemente menos exigentes em relação aos recursos computacionais.
- O consumo de banda no gerente foi reduzido.
- A adoção do SNMP e HTTP facilitou a portabilidade do sistema.

3.5 Kätker e Paterok

O artigo descrito nesta seção não trata originalmente de gerenciamento proativo. Por outro lado, o artigo possui conceitos aplicáveis ao tema que justificam a sua incorporação ao trabalho.

[Kätker e Paterok, 1997] apresentam um breve estudo sobre quatro métodos de correlação de alarmes: sistemas especialistas, modelo de propagação de falhas, modelagem baseada em casos e em técnicas transversas. Os autores apresentam também as características mínimas para localização de falhas e correlação de alarmes, e uma nova proposta de algoritmo baseada em técnica transversa.

Segundo [Kätker e Paterok, 1997] as características mínimas são:

- Integração a infra-estrutura de gerência: o algoritmo deve estar integrado à planta de modo a acessar as facilidades oferecidas pelos recursos de rede.

- Flexibilidade: o algoritmo deve ser capaz de lidar com as mudanças de topologia e alterações nas configurações dos equipamentos de rede, tais como: atualizações de *software* e *upgrade.*
- Desempenho e paralelismo: Normalmente requisições por informações sobre o estado da rede gastam mais tempo que a correlação em si. Neste caso é importante executar o processamento destas mensagens em paralelo.
- Distribuição funcional e combinação de técnicas: O algoritmo deve ser facilmente portável para diferentes arquiteturas e deve permitir a sua execução em conjunção com outras técnicas.
- Ser robusto: o algoritmo deve ser robusto quando estiver trabalhando com dados incompletos causados por falhas na rede.

O algoritmo proposto pelos autores foi patenteado e adotado pela IBM nas soluções para ambientes TMN *(Telecommunications Management Network).* O processamento é realizado em duas etapas (Figura 2): pesquisa horizontal e pesquisa vertical. A pesquisa horizontal é iniciada quando há a identificação de uma falha. Esta etapa consiste na procura do recurso que possivelmente originou o problema. Tendo sido descoberta a possível origem do problema é feita uma pesquisa vertical dentro do recurso sob suspeita. Esta pesquisa consiste em uma varredura nos sub-sistemas para a determinação e verificação da origem da falha. Concluída esta etapa, a informação é passada para o gerente que a correlaciona com os demais alarmes e termina a identificação do alarme.

Os autores concluem o trabalho afirmando que o algoritmo apresentado é de simples implementação, eficiente na localização da origem de falhas e facilmente integrável a outros métodos de correlação.

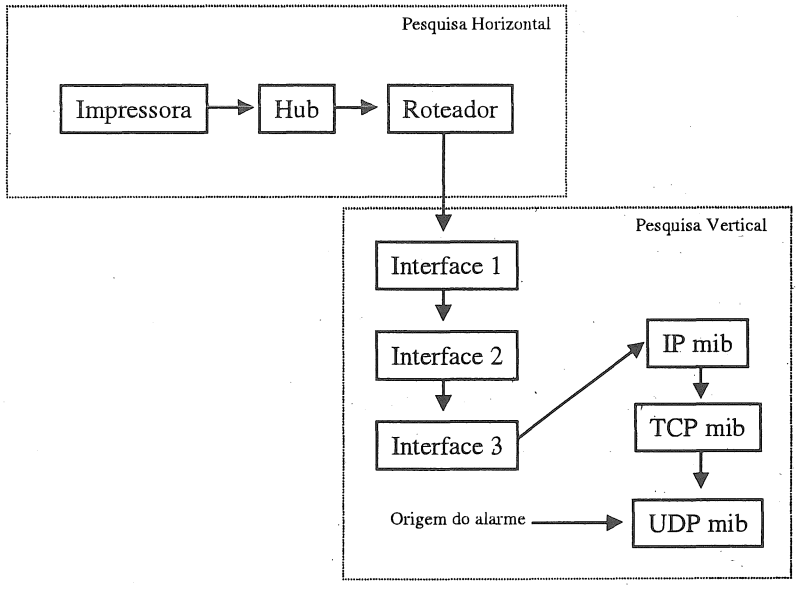

Figura 2 - Algoritmo para identificação de origem de falhas

3.6 Consolidação

A proposta de [Cruz et al., 1997] é uma evolução do trabalho de [Rocha e Westphall, 1997] em função da adoção de um ambiente de desenvolvimento e testes de sistemas especialistas. Os trabalhos desenvolvidos por [Hood e Ji, 1998] e [Grimes e Adley, 1997] apesar de abordarem escopos diferentes apresentam como característica comum a descentralização do conhecimento. Esta característica é desejável para sistemas de gerência de redes geograficamente dispersas onde o atraso na comunicação entre nodos não é desprezível.

Os cinco trabalhos relacionados abordam a necessidade de se integrar novas heurísticas às suas implementações. Tal fato pode ser atribuído a incapacidade de uma heurística ser eficiente para todos os casos de gerência.

A implementação de [Kätker e Paterok, 1997] apresenta um algoritmo para correlação de alarmes que pode ser utilizado em gerenciamento proativo. Por exemplo, dado um comportamento anormal em um elemento de rede, pode-se realizar uma pesquisa vertical nos diversos elementos deste recurso de modo a determinar a origem exata do possível problema.

4. Gerenciamento proativo nas empresas

Esta seção apresenta algumas soluções comerciais disponíveis no mercado que utilizam como base o gerenciamento proativo. A seção 4.1 apresenta a solução da AT&T no gerenciamento do seu *backbone*. A seção 4.2 apresenta os *softwares TrafficDirector* e Cisco *Netsys Connectivity Service Manager* desenvolvidos pela Cisco. Na seção 4.3 são descritas soluções 3Com. A seção 4.4 apresenta as soluções *AdvancedStack Assistant* e *NetMetrix* da HP. Finalmente, na seção 4.5 é realizada uma consolidação das quatro seções anteriores.

4.1 AT&T

A [AT&T] possui um *backbone* interligando 250 países. O *backbone* é composto por enlaces de fibra-ótica, microondas e satélites, e disponibiliza serviços para voz e dados. Com o objetivo de gerenciar esta infra-estrutura foi desenvolvido um sistema com as seguintes premissas:

- Atendimento do maior número de chamadas na primeira tentativa.
- Determinação do padrão de tráfego do usuário de forma a alocá-lo em um canal mais apropriado.
- Capacidade de previsão de eventos com o objetivo de reduzir o impacto na rede, por exemplo: promoções interativas na TV.
- Monitoramento constante de todos os recursos da rede, reduzindo assim problemas potenciais.
- Canal direto com a CNN para a imediata notificação de desastres naturais (tempestades, furacões, terremotos, etc.). Tais eventos podem implicar em dificuldades nas ligações de longa distância, permitindo que, ao ser detectado um problema contramedidas possam ser tomadas rapidamente.

Para isto foram criados três centros principais de gerência de redes responsáveis pelo completo monitoramento da rede. Segundo a [AT&T], as informações destes centros são atualizadas a cada cinco minutos e dependendo do tipo da informação a cada 30 segundos. O artigo afirma que a confiabilidade das conexões telefônicas obtida desde a implantação de tais centros supera a 99.98%, sendo 173 o número médio de ligações não completadas em um milhão de tentativas.

4.2 Cisco

A Cisco possui duas soluções para serem usadas com seus equipamentos. A ferramenta *TrafficDirector* [Cisco a] atua como uma extensão para um console RMON *(Remote Monitoring)* provendo um conjunto de ferramentas para análise de tráfego. Os gráficos gerados pelo *software* fornecem informações úteis no planejamento de capacidade. Deste modo, é possível a atuação proativa do administrador na rede.

O software *Netsys* [Cisco b] é apresentado como uma ferramenta para gerenciamento de configuração, desempenho e falhas na rede. A ferramenta apresenta as seguintes funções:

- Capacidade de armazenar configurações dos elementos de rede, verificando-as temporariamente.
- Distribuição de relatórios sobre a saúde relativa dos recursos da rede.
- Determinação de problemas de roteamento e *status* operacional dos roteadores.

- Ambiente de testes para alterações na rede.

Em relação a gerência proativa a ferramenta é capaz de:

- Prevenir o uso ineficiente de enlaces WAN através da verificação da configuração dos roteadores.
- Reduzir o tempo de projeto da rede em função da plataforma de testes.

4.3 3Com

A [3Com a] oferece suporte a gerenciamento proativo nas suas soluções em *hardware* através de sete grupos RMON. Esses grupos auxiliam no gerenciamento de tráfego e na previsão de capacidade.

A 3Com produz o *software Transcend Enterprise Manager'97* [3Com b]. Esta ferramenta oferece um ambiente de gerência que permite o monitoramento das condições da rede (desempenho, falhas e configuração). A ferramenta possui um módulo de gerência proativa para controle do desempenho onde são definidos limites de operação da rede.

4.4 HP

A ferramenta *AdvancedStack Assistant* [HP a] possibilita o gerenciamento proativo de *hubs* e *switches* HP. O *software* determina o perfil de tráfego e utilização de cada máquina indicando, quando necessário, sua atualização. A ferramenta implementa controle automático de tráfego e é capaz de corrigir automaticamente pequenas falhas, tais como: quedas de conexão e número excessivo de *broadcasts*. O *software* disponibiliza uma série de gráficos de utilização que auxiliam o administrador na tomada de decisões.

A outra solução da HP é uma extensão do *OpenView*. O HP *NetMetrix* [HP b] oferece gerenciamento proativo de desempenho. Através do monitoramento do tráfego dos diversos dispositivos de rede é possível determinar um perfil de tráfego / utilização e consequentemente determinar os limites para degradação dos serviços. Assim sendo, o sistema é responsável por informar ao administrador quando um recurso de rede se aproxima dos limites de degradação permitindo que este possa planejar com antecedência a atualização do recurso.

4.5 Consolidação

As soluções desenvolvidas pelos fabricantes citados nesta seção abordam, principalmente, a gerência de desempenho. Isto pode ser atribuído às seguintes dificuldades:

- O problema da localização da origem de uma falha na rede é classificado como NP-Completo [Katzela e Shwartz,1993].
- A correlação de alarmes é dependente da arquitetura da rede. Este fato dificulta o desenvolvimento de *softwares* para ambientes heterogêneos.

As propostas da Cisco são voltadas para o monitoramento dos seus roteadores, o que limita a sua utilização. As propostas da HP e 3Com têm por objetivo o gerenciamento de todos os aspectos da rede, porém a gerência proativa é efetivamente implementada apenas no gerenciamento de desempenho.

A solução da AT&T apresenta-se como a mais completa, sendo a única que implementa efetivamente a gerência proativa. Esta situação ocorre em função da necessidade de se oferecer serviços de qualidade com baixo custo em um mercado competitivo. Tal característica justifica o elevado gasto no desenvolvimento de um sistema deste porte.

5. Conclusões

O quadro a seguir (Figura 3) apresenta a distribuição dos artigos em função da camada de atuação no modelo Internet e a área de gerência abordada:

	Trabalhos	Área de Conhecimento				
		Configuração	Contabilização	Desempenho	Falhas	Segurança
Acadêmicos	Cruz et al.			Controla o desempenho dos dispositivos da rede ATM	Utiliza um sistema especialista para fazer a correlação de alarmes	
	Grimes e Adley			Utiliza agentes móveis com o objetivo de reduzir o overhead no sistema	Defende que agentes móveis autônomos não dependem do nó central para tomada de decisões em caso de falhas	
	Hood e Ji				Utiliza redes bayesianas e agentes móveis para determinar a origem das falhas	
	Kätker e Paterok				Apresenta um algoritmo para correlação de alarmes	
	Rocha e Westphall	Controla a configuração dos equipamentos		Adota um sistema especialista para controle do desempenho	Adota um sistema especialista para controle das falhas	
Comerciais	AT&T	Altera sob demanda a configuração da rede	Executa a tarifação	Otimiza a utilização dos canais em função do perfil de utilização	Realoca recursos em função de catástrofes	Controla o acesso a rede
	Cisco TrafficDirector			Define limites de operação para os equipamentos. Possibilita a atuação proativa do administrador na rede	Define limites de operação para os equipamentos. Possibilita a atuação proativa do administrador na rede	
	Cisco Netsys	Determina e verifica as configurações dos equipamentos Cisco		Verifica o uso eficiente dos canais de comunicação	Trata problemas de roteamento e falhas em equipamentos Cisco	
	3Com			Atua a partir da definição por parte do administrador de faixas de operação		
	HP Advanced Stack			Permite controlar o tráfego porém sem atuar efetivamente	Corrige automaticamente pequenas falhas em *Hubs* e *Switches* HP	
	HP NetMetrix			Possibilita a atuação proativa do administrador na rede		

Figura 3 - Quadro de distribuição dos trabalhos

A partir deste quadro é possível verificar que a maioria das implementações comerciais abordam a gerência de desempenho enquanto nos trabalhos acadêmicos a ênfase é divida entre a gerência de falhas e de desempenho. Isto pode ser atribuído às dificuldades na localização de falhas em um ambiente de rede, o que dificulta a implementação de uma solução comercial genérica. Outro indicador desta dificuldade é a existência em algumas implementações [Cisco a, HP b] do conceito de atuação proativa do gerente de rede. Neste caso, ao invés do software executar as contramedidas necessárias, este apenas indica os problemas ao gerente que deve então agir proativamente na rede.

O gerenciamento proativo é um aspecto importante que deve ser considerado nas novas implementações em gerência de redes. A adoção desta tecnologia apresenta como vantagens:

- Redução do *downtime*: a rede passa a apresentar menores tempos de inoperância em função da capacidade de se prever falhas.
- Alocação eficiente de recursos: a análise do comportamento da rede permite a determinação exata das necessidades de cada recurso da rede permitindo uma melhor distribuição de equipamentos.
- Previsão de capacidades: a análise dos perfis de tráfego/utilização auxilia na previsão das necessidades futuras da rede. Deste modo consegue-se evitar perdas de produtividade em função da saturação prematura de um dos recursos.

A gerência proativa apresenta porém uma série de dificuldades:

- Dependência da topologia e das soluções adotadas: os perfis de utilização, tráfego e falhas são dependentes da solução adotada. Sendo assim, torna-se difícil implementar uma ferramenta genérica de gerência.
- Dificuldades de implementação: a necessidade de implementar gerentes inteligentes, diferentes técnicas de correlação de alarmes e de determinação de comportamento dificultam o desenvolvimento deste tipo de aplicação
- Dificuldades de determinação dos parâmetros de operação da rede: a determinação dos parâmetros de operação constitui um processo lento e que depende da análise dos dados de um longo período de tempo. Nem sempre estes dados estão disponíveis, o que dificulta a execução desta etapa.

Agradecimentos

Este trabalho foi apoiado em parte pelos convênios FAPEMIG SHA 250/94, TEC 609/96 e CNPq 522618/96-0

Referências bibliográficas

[3Com] *SuperStack II Switch 1000.* Disponível em http://www.3com.com/products/dsheets/400324.html

[AT&T] *The AT&T Worldwide Intelligent Network – 1998.* Disponível em http://www.att.com/network

[Cisco a] *TrafficDirector Version 4.1.* Disponível em http://www.cisco.com/warp/public/734/traffdir/tdir_ds.htm.

[Cisco b] *Proactive Network Management with Cisco Netsys Connectivity Service Manager.* Disponível em http://www.cisco.com/warp/public/734/nslms/proac_wp.htm.

[Cruz et al., 1997] Fernando A. S. Cruz, Mirela S. M. A. Notare, Fernando Gauthier, Bernardo G. Riso, Carlos B. Westphall. *Uso de Inteligência Artificial na Implementação de um Sistema de Gerência Proativo para Redes ATM.* XXIII Conferência Latino-americana de informática, 1997.

[Grimes e Adley, 1997] Garry Grimes, Brian P Adley. *Intelligence Agents for Network Fault Diagnosis and Testing.* Integrated Network Management V, 1997.

[Hood e Ji, 1998] Cynthia S. Hood, Chuanyi Ji. *Intelligent Agents for Fault Detection.* IEEE Internet Computing, Volume 2, Number 2, March April, 1998.

[HP a] *HP Increases Network Manager Control with New Proactive Networking Solution.* Disponível em http://www.hp.com.

[HP b] *Moving from Reactive to Guaranteed Network Services.* http://www.hp.com.

[Kätker e Paterok, 1997] S. Kätker, M. Paterok. *Fault Isolation nad Event Correlation for Integrated Fault Management.* Integrated Network Management V, 1997.

[Katzela e Shwartz,1993] I. Katzela, M. Shwartz. *Schemes for Fault Identification in Communication Networks.* IEEE International Conference on Communications, 1993.

[Meira e Nogueira, 1997] Dilmar M. Meira, José Marcos S. Nogueira. *Métodos e Algoritmos para Correlação de Alarmes em Redes de Telecomunicações.* Anais 15º Simpósio Brasileiro de Redes de Computadores, 1997. Disponível em http://www.sis.dcc.ufmg.br.

[Rocha e Westphall, 1997] Marco A. Rocha, Carlos B. Westphall. *Proactive Management of Computer Networks Using Artificial Intelligence Agents and Techniques.* Integrated Network Management V, 1997.

[Soares et al., 1995] Luiz Fernando G. Soares, Guido Lemos, Sérgio Colcher. *Redes de Computadores: das LANs, MANs e WANs às redes ATM.* 2.ed. rev. e ampliada. Campus, 1995.

[Stallings, 1993] William Stallings. *SNMP, SNMPv2 and CMIP: The Practical Guide to Network Management Standard.* Addison Wesley, 1993.

[Tanembaum, 1996] Andrew S. Tanembaum. *Computer Networks.* 3rd Edition. Prentice Hall, 1996.