Métodos e Algoritmos Para Correlação de Alarmes em Redes de Telecomunicações

*Dilmar Malheiros Meira** *José Marcos S. Nogueira*†

Laboratório de Redes de Computadores e Sistemas Distribuídos
Departamento de Ciência da Computação
Universidade Federal de Minas Gerais — UFMG
Belo Horizonte, MG
E-mail: {dilmar, jmarcos}@dcc.ufmg.br
http://www.sis.dcc.ufmg.br

Resumo

Este documento conceitua o problema de correlação de alarmes em uma rede de telecomunicações, classificando as principais abordagens encontradas na literatura de acordo com os métodos e algoritmos adotados no processo de correlação.

Abstract

This paper presents the main concepts on the problem of alarm correlation on telecommunications networks, and classifies the main approaches found in the literature, according to the methods, strategies and algorithms used by the correlation process.

1 Introdução

Gerência de redes de telecomunicações envolve a *transferência* e o *processamento* de informações de gerência, com o objetivo de auxiliar uma empresa de telecomunicações a conduzir com eficiência o seu negócio [ITU-T, 1992a]. Até há pouco tempo, a maior parte do esforço dispendido no desenvolvimento de gerência de redes vinha sendo destinada aos aspectos relacionados à transferência de informações. Neste contexto se encaixa a grande polêmica em torno das virtudes e limitações dos protocolos CMIP e SNMP [Gering, 1993]. Por mais importante, necessária e complexa que seja, coleta de informações não é gerência de rede, mas apenas um pré-requisito para essa gerência.

Segundo o ITU-T, setor normativo de telecomunicações da União Internacional de Telecomunicações, *gerência de falhas* engloba detecção, isolação e correção de falhas [ITU-T, 1992b]. Qualquer dessas três funções só pode ser realizada a partir da *adição de valor* [Mansfield *et al.*, 1993] aos dados brutos coletados da planta.

Através de *correlação de alarmes*, dados brutos são interpretados e analisados, levando em consideração um conjunto de critérios pré-estabelecidos, ou definidos dinamicamente em função do processo de gerência. A correlação adiciona valor aos alarmes originais e é um importante mecanismo de gerência de redes.

Ao reduzir o tempo necessário para a identificação das falhas causadoras dos alarmes, permitindo a rápida restauração dos serviços afetados, a implantação de correlação de

*Aluno do Curso de Doutorado em Ciência da Computação da UFMG. Engenheiro da TELEMIG — Telecomunicações de Minas Gerais S.A.

†Professor Adjunto do Departamento de Ciência da Computação da UFMG

alarmes em um centro de operação americano típico pode trazer benefícios anuais de até US$1 milhão [Nygate, 1995]. A importância deste assunto é reconhecida pelo ITU-T, que classifica a correlação de alarmes como um dos problemas a serem resolvidos para que um sistema de gerência de redes produza os resultados que dele se deseja. Apesar desta importância, o ITU-T ainda não definiu sua posição quanto à matéria, que se encontra aberta a estudos [ITU-T, 1995].

Correlação de alarmes é um tópico complexo, que pode ser estudado sob diversas perspectivas. Muito tem sido escrito sobre o assunto, porém o conhecimento existente encontra-se disperso na literatura, que carece de uma visão panorâmica sobre a matéria.

Os objetivos deste artigo são: (1) estabelecer os principais conceitos ligados a correlação de alarmes e diagnóstico de falhas em uma rede de telecomunicações; (2) reunir as principais abordagens existentes na literatura sobre correlação de alarmes em redes de telecomunicações e (3) classificá-las segundo os métodos e algoritmos utilizados.

Segundo [Tanenbaum, 1996], uma rede de computadores é um conjunto de computadores autônomos interconectados, isto é, aptos a trocarem informação entre si. Desta forma, muitos dos sub-sistemas de telecomunicações modernos (por exemplo, as redes de sinalização, as redes inteligentes e as redes de gerência) podem ser vistos como grandes redes de computadores. Portanto, a opção pelo estudo de correlação de alarmes em uma rede de telecomunicações não implica em perda de generalidade em relação ao estudo do assunto em redes de computadores.

A seção 2 deste trabalho reúne os conceitos mais importantes sobre correlação de alarmes e diagnóstico de falhas em uma rede de telecomunicações; a seção 3 apresenta os principais métodos, estratégias e algoritmos encontrados na literatura; a seção 4 introduz alguns critérios para comparação entre essas abordagens; a seção 5 traz algumas considerações finais.

2 Correlação de Alarmes

Um objeto gerenciado, que pode ser visto como uma representação de um recurso real, pode emitir *notificações* em resposta à ocorrência de algum *evento* interno a ele. As notificações, bem como as informações nelas contidas, são definidas pela classe de objetos gerenciados da qual o objeto gerenciado é uma instância [ITU-T, 1992c]. Uma notificação pode ser transmitida para fora do objeto gerenciado, ou simplesmente armazenada internamente ao objeto [ITU-T, 1992e].

Relatórios de eventos são utilizados para, através do uso de protocolos de comunicação, reportar a ocorrência de eventos em um objeto gerenciado [ITU-T, 1991].

Dá-se o nome de *falha* à causa de um mau funcionamento. Falhas são responsáveis por dificultar ou impedir o funcionamento normal de um sistema e se manifestam através de *erros*, ou seja, desvios em relação à operação normal do sistema.

Um *alarme* consiste de uma notificação sobre a ocorrência de um evento específico, que pode ou não representar um erro. Um *relatório de alarme* é um tipo de relatório de evento, usado no transporte de informações de alarme [ITU-T, 1992d].

Alguns autores [Kehl e Hopfmüller, 1993] definem *correlação* como um processo no qual se cria um conjunto mínimo de hipóteses de falhas para um dado conjunto de alarmes. Esta definição pode ser adequada para o contexto de *diagnóstico de falhas* (v. item 2.1) mas, considerando que um alarme nem sempre está associado a uma falha, prefere-se adotar a definição dada por [Jakobson e Weissman, 1993], segundo a qual *correlação de alarmes* consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais. A correlação geralmente tem como objetivo reduzir a quantidade de notificações de alarmes transferidas aos operadores do sistema de gerência de rede, aumentando o conteúdo semântico das notificações

resultantes.

Correlação de alarmes pode ser aplicada a qualquer das cinco áreas funcionais de gerência definidas pelo ITU-T, quais sejam, falhas, configuração, contabilização, desempenho e segurança [ITU-T, 1992b]. Contudo, a maioria das aplicações encontradas na literatura está na área de gerência de falhas, que é a mais elementar e, por isto mesmo, talvez a mais importante. Devido ao grande volume de informações envolvidas, existem outras áreas onde a correlação de alarmes pode ser útil. Gerência de tráfego, por exemplo, é uma aplicação que demanda a coleta e o processamento de informações, em tempo real, com o objetivo de detectar anomalias nos padrões de tráfego da rede e tomar as providências necessárias para remediá-las. Dentre as anomalias ou *condições de exceção* mais importantes destacam-se as sobrecargas aleatórias, os troncos *"killer"* — que sistematicamente aceitam as chamadas que lhes são oferecidas e as libera (*mata*) logo em seguida — e as sobrecargas de tráfego geradas por eventos excepcionais, tais como catástrofes, promoções de vendas por telefone e datas especiais [Goodman *et al.*, 1993].

O principal requisito para se fazer gerência de falhas de forma integrada é a disponibilização, em um centro de gerência, de informações sobre o funcionamento da rede, em tempo real. As anormalidades que ocorrem durante a operação da rede provocam a emissão automática de notificações de alarmes, as quais são recebidas no centro de gerência de rede. A partir das notificações de alarmes recebidas, o operador humano deve tentar identificar a falha ocorrida e, se necessário, emitir um *bilhete de anormalidade*, que é utilizado como referência para o acionamento das equipes de manutenção. Uma vez sanado o problema, o bilhete de anormalidade é "fechado", ficando disponível apenas para consulta.

Com o crescimento da planta gerenciada, estima-se que, a médio prazo, o centro de gerência de uma empresa regional de médio porte estará recebendo dezenas de milhares de notificações de alarmes por dia, o que tornará praticamente inviável o processamento "manual" de todas elas [Nygate, 1995].

Além disso, muitas das notificações recebidas não contêm informação original. De fato, a ocorrência de uma única falha na rede supervisionada às vezes resulta no recebimento de múltiplas notificações. Diversos fatores contribuem para esta situação [Houck *et al.*, 1995]:

1. Um dispositivo pode gerar diversos alarmes em decorrência de uma única falha;
2. A falha pode ser intrinsecamente intermitente, o que implica no envio de uma notificação a cada nova ocorrência;
3. A falha de um componente pode resultar no envio de uma notificação de alarme a cada vez que se invoca o serviço prestado por esse componente;
4. Uma única falha pode ser detectada por múltiplos componentes da rede, cada um deles emitindo uma notificação de alarme;
5. A falha de um dado componente pode afetar diversos outros componentes, causando a propagação da falha.

Ainda que, a princípio, a correlação possa ser feita "manualmente" pelos operadores dos centros de gerência de rede, no contexto deste trabalho a expressão *correlação de alarmes*, ou a expressão equivalente *"correlação de eventos"*, subentende o uso de recursos computacionais no processo de correlação.

2.1 Diagnóstico de Falhas

Diagnóstico de Falhas é uma etapa no processo de gerência de falhas que consiste em descobrir qual a causa original para os *sintomas* (representados pelos alarmes) recebidos.

Antes de se chegar à causa original, pode ser necessária a formulação de um conjunto de hipóteses de falhas, as quais precisarão ser validadas através de testes.

É desejável que um sistema para diagnóstico de falhas possua um modelo da configuração gerenciada, processe o fluxo de alarmes em tempo real e seja capaz de trabalhar com dados incompletos. Além disto, espera-se que ele seja capaz de identificar mudanças na aparência e na importância dos problemas em função do tempo (e.g., horário, dia da semana, estação do ano), de separar causa de efeitos e resolver os problemas por ordem de severidade (i.e., os problemas mais graves devem ter prioridade). Na seleção dos testes a serem aplicados, o sistema deve escolher os mais baratos e mais eficazes. Na medida do possível, os testes diagnósticos devem ser automatizados. Finalmente, é desejável que o sistema consiga, de alguma forma, interpretar os resultados dos testes [Sutter e Zeldin, 1988].

O problema de localização de falhas é NP-completo [Katzela e Schwartz, 1995], o que significa, no caso geral, que não existe um algoritmo polinomial que o resolva. Entretanto, através de heurísticas [Pearl, 1984], em alguns casos pode-se desenvolver algoritmos polinomiais que deem soluções aproximadas ou, em outros casos, que deem uma solução correta, com uma dada probabilidade [Katzela *et al.*, 1995].

As necessidades de recebimento e armazenamento centralizado de alarmes, de conhecimento da configuração do sistema gerenciado no momento da falha e de conhecimento sobre como uma falha em um componente afeta componentes adjacentes na configuração são algumas das barreiras que precisam ser ultrapassadas antes que uma solução prática para o problema de correlação de alarmes possa ser implementada. No caso mais geral, a correlação pode demandar outras informações, tais como resultados de testes executados na rede, dados obtidos em bancos de dados externos e junto aos usuários. A dificuldade na obtenção destas informações constitui um obstáculo à implementação comercial de correlação de alarmes e justifica o fato de que, dentre as diversas abordagens que tem sido propostas, poucas têm aplicações práticas na gerência integrada de redes de telecomunicações.

3 Métodos e Algoritmos

A complexidade característica das aplicações de correlação de alarmes torna este um campo ideal para a utilização de *inteligência artificial* (AI).

AI pode ser definida como um ramo da ciência no qual se propõem modelos para o estudo de computações dos tipos usualmente executados pelo cérebro [Charniak e McDermott, 1986]. Mesmo tendo raízes na ciência da computação, a disciplina Inteligência Artificial possui intersecção com diversos outros campos, tais como filosofia, linguística, psicologia, matemática, física, estatística e neurologia. É uma ciência em plena infância, o que explica por que ela se desenvolve muito mais rapidamente que a maioria das outras ciências [Ginsberg, 1993].

Dentre as diversas abordagens de inteligência artificial, algumas se caracterizam por utilizarem uma *base de conhecimento* contendo fatos e estratégias para solução de problemas em um estreito campo de conhecimento, construída a partir da experiência de especialistas humanos. Sistemas que adotam estas abordagens são genericamente conhecidos como *sistemas especialistas* ("expert systems") ou *sistemas baseados em conhecimento* ("knowledge-based systems"), às vezes também denominados *sistemas de produção* ou *sistemas baseados em regras* ("Rule-Based" – RB), em alusão às técnicas mais utilizadas na sua implementação [DeSalvo, 1988] [Charniak e McDermott, 1986] . Os principais conceitos pertinentes a sistemas especialistas, incluindo os mecanismos de controle e de aquisição e representação do conhecimento, são explorados em [Brownston *et al.*, 1986] e [Cronk *et al.*, 1988], que apresentam exemplos de programas, desenvolvidos na linguagem

OPS5 (Official Production System, Version 5).

A seguir são apresentadas as principais abordagens encontradas na literatura sobre correlação de alarmes. Algumas dessas abordagens utilizam paradigmas tradicionais de AI, outras aplicam princípios definidos em lógicas não-convencionais [Smets *et al.*, 1988], enquanto que umas tantas outras adotam métodos *ad hoc* para o tratamento do problema.

3.1 Correlação Baseada em Regras

Das diversas propostas apresentadas na literatura sobre correlação de alarmes em sistemas de telecomunicações, uma parcela significativa constitui-se de variações em torno da clássica abordagem baseada em regras (RB). Nesta abordagem, o conhecimento geral sobre determinada área está contido em um conjunto de regras e o conhecimento específico, relevante para uma situação particular, constitui-se de fatos, expressos através de asserções e armazenadas em um banco de dados. Uma regra consiste de duas expressões — fórmulas bem formadas do cálculo de predicados [Nilsson, 1980] — ligadas por um conectivo de implicação ($\Rightarrow$), e que operam sobre um banco de dados global. O lado esquerdo de cada regra contém um pré-requisito que precisa ser satisfeito pelo banco de dados para que a regra seja aplicável. O lado direito descreve a ação a ser executada se a regra for aplicada. A aplicação de uma regra altera o banco de dados.

Todo sistema RB (ou *sistema de produção*) possui uma estratégia de controle que determina em que ordem as regras aplicáveis serão aplicadas e que pára a computação quando uma condição de término é satisfeita pelo banco de dados.

Existem dois modos de operação em um sistema de produção. O primeiro deles é o modo *direto* ("forward"), no qual parte-se de um estado inicial e se constrói uma seqüência de passos que leva até a solução do problema ("goal"). Em se tratando de um sistema de diagnóstico de falhas, as regras seriam aplicadas a um banco de dados contendo todos os alarmes recebidos, até se atingir uma condição de término envolvendo uma falha. No segundo modo de operação, denominado modo *reverso* ("backward"), parte-se da configuração correspondente à solução do problema e se constrói uma seqüência de passos que leva até a configuração correspondente ao estado inicial. Tomando-se novamente como exemplo um sistema de diagnóstico de falhas, as regras seriam aplicadas a um banco de dados contendo todas as falhas possíveis, até que fosse atingida uma condição de término na qual todos os alarmes recebidos estivessem presentes. Um mesmo conjunto de regras pode ser usado para os dois modos de operação [Rich, 1983].

Em comparação com os programas tradicionais, que contém em seu código tanto o conhecimento especializado quanto as informações de controle — o que contribui para torná-los extremamente complexos e de difícil manutenção — um sistema especialista baseado em regras é mais simples, mais modularizado e mais fácil de manter, por ser organizado em três níveis [Cronk *et al.*, 1988]:

a) Uma máquina de inferência, que contém a estratégia para resolver uma determinada classe de problemas;

b) Uma base de conhecimento, contendo um conjunto de regras com o conhecimento sobre uma tarefa específica, ou seja, uma instância daquela classe de problemas;

c) Uma memória de trabalho, contendo os dados sobre o problema sendo tratado.

A despeito das vantagens que apresenta em relação aos programas tradicionais, os sistemas baseados em regras apresentam algumas limitações no que se refere à aquisição do conhecimento necessário, que se baseia, a princípio, em entrevistas com especialistas humanos. Este procedimento é demorado, caro e sujeito a erros, o que tem incentivado

pesquisas no sentido de automatizá-lo e torná-lo mais rápido, através de técnicas de *aprendizado* ("machine learning") [Michalski *et al.*, 1983] [Goodman e Latin, 1991].

Outra limitação destes sistemas é o não aproveitamento de experiências passadas no processo dedutivo, ou seja, a falta de "memória". Assim, um sistema puramente baseado em regras que tenha disparado milhares de regras para, a partir de um dado conjunto de alarmes, deduzir a ocorrência de determinada falha, irá disparar novamente todas aquelas regras sempre que for submetido ao mesmo conjunto de alarmes, chegando mais uma vez à mesma conclusão. O programa não se "lembra" da ocorrência de uma situação similar no passado.

Por não fazer uso de experiências passadas, os sistemas baseados em regras estão sujeitos a repetir sempre os mesmos erros, o que contribui negativamente para a precisão e o desempenho desses sistemas.

Tendo seu conhecimento limitado às regras do seu banco de dados, o sistema não consegue lidar com as situações nas quais estas regras não se aplicam. Isto afeta sua robustez [Lewis e Dreo, 1993]; o sistema pode ficar sem alternativas ante a muitas situações comuns de um ambiente de gerência integrada de rede.

Em domínios que se modificam rapidamente, como é o caso das redes de telecomunicações, sistemas baseados em regras tendem rapidamente a se tornarem obsoletos [Lewis, 1993]

3.2 Lógica Difusa

Devido à complexidade das redes gerenciadas, nem sempre é possível construir-se modelos precisos dessas redes, nos quais sejam evidenciadas todas as situações em que a ocorrência de um dado conjunto de alarmes indica falha de um determinado equipamento.

O conhecimento sobre as relações de causa e efeito entre falhas e alarmes é geralmente incompleto. Além disto, freqüentemente alguns dos alarmes gerados por uma falha não são tornados disponíveis ao sistema de correlação, em tempo hábil, em virtude de perda ou atraso no percurso desde o elemento de rede que lhes deu origem. Finalmente, devido ao fato de que a configuração muda frequentemente, quanto mais detalhado for um modelo, mais rapidamente ele ficará desatualizado.

Uma grande dificuldade, muitas vezes, consiste na imprecisão das informações fornecidas pelos especialistas. Num exemplo hipotético, um especialista em gerência de rede poderia formular as seguintes regras:

1. Se o tráfego na rota A estiver *muito alto* e o tráfego na rota B estiver *normal* então desvie 1/4 do tráfego da rota A para a rota B;

2. A ocorrência do alarme C *às vezes* indica falha do equipamento D.

As expressões "muito alto", "normal" e "às vezes" são inerentemente imprecisas e não podem ser diretamente incorporadas à base de conhecimento de um sistema RB convencional.

Lógica difusa ("fuzzy logic") é uma alternativa para lidar com a incerteza e a imprecisão que caracterizam algumas aplicações de gerência de redes de telecomunicações.

De acordo com [Zadeh, 1988], a lógica difusa contém, como casos especiais, o sistema lógico tradicional, os sistemas lógicos multivalorados, a teoria das probabilidades e a lógica probabilística. Por outro lado, apesar de ser possível constatar empiricamente que um dado sistema baseado em lógica difusa opera de acordo com que dele se esperava, ainda não existem ferramentas que permitam provar, *a priori*, que esse sistema funciona [Meech e Kumar, 1994], o que indica que os conceitos introduzidos por [Zadeh, 1965] ainda não contam com suficiente respaldo matemático.

Alguns pesquisadores argumentam que todos os problemas que podem ser resolvidos através de lógica difusa podem igualmente ser resolvidos através de modelos probabilísticos (e.g., redes bayesianas — cf. item 3.3), com a vantagem de se contar, neste último caso, com uma sólida base matemática, o que falta à lógica difusa [Luna, 1994].

O conceito básico por trás da lógica difusa são os *conjuntos difusos* ("fuzzy sets"). Na lógica clássica, um conjunto A apresenta a propriedade de que, dado um elemento X, a expressão "X pertence a A" sempre assume um dentre dois valores possíveis: *verdadeiro* ou *falso*. Em se tratando de conjuntos difusos, cada elemento X tem, em relação ao conjunto, um certo *grau de pertinência*, que pode assumir qualquer valor entre 0 (quando, definitivamente, o elemento não pertence ao conjunto) e 1 (quando certamente o elemento é um membro do conjunto). O conceito de conjunto difuso traz consigo a novidade de que uma proposição qualquer não precise mais ser apenas verdadeira ou falsa, mas que possa ser parcialmente verdadeira, em qualquer grau na escala de 0 a 1.

Através de uma álgebra especial, são definidas diversas operações (p.ex., complementação, interseção e união) sobre conjuntos difusos.

Sistemas especialistas difusos ("fuzzy systems") permitem que as regras sejam diretamente formuladas utilizando *variáveis linguísticas* do tipo *"muito alto"* ou *"normal"*, o que simplifica bastante o desenvolvimento do sistema.

Numerosas aplicações de sistemas difusos têm sido implementadas, em diversas áreas, tais como: planejamento estratégico [Hall, 1987], engenharia de minas [Meech e Jordon, 1993], geologia [Lebailly *et al.*, 1987], medicina [Henkind *et al.*, 1987], ciências ambientais [Veiga e Meech, 1994], engenharia elétrica [Chen e Rao, 1993] e gerência de redes [Lirov, 1993].

Uma boa introdução aos sistemas difusos é apresentada em [Negoita, 1984]. Os aspectos teóricos dos sistemas especialistas baseados em lógica difusa são explorados em [Gupta *et al.*, 1985], que também traz diversas aplicações desses sistemas.

3.3 Redes Bayesianas

Redes Bayesianas [Charniak, 1991] [Pearl, 1991] [Deng *et al.*, 1993] [Kirsch e Kroschel, 1994] constituem uma interessante abordagem para tratamento de incerteza. Através delas é possível a realização de inferências mesmo quando as informações disponíveis são incompletas e imprecisas. Uma rede bayesiana é um grafo acíclico dirigido no qual cada nodo representa uma variável aleatória à qual são associadas as *probabilidades condicionais subjetivas*, dadas todas as possíveis combinações de valores das variáveis representadas pelos nodos predecessores diretos. Uma probabilidade subjetiva expressa o *grau de crença* ("degree of belief") de um especialista em relação à ocorrência de um dado evento, a partir das informações de que esta pessoa dispõe até o momento [Henrion *et al.*, 1991]. O uso de probabilidades subjetivas muitas vezes é o único recurso, em situações onde a obtenção de dados analíticos ou experimentais é muito difícil, ou mesmo impossível.

Dada uma rede Bayesiana e um conjunto de *evidências* — isto é, nodos cujas correspondentes variáveis foram instanciadas — é possível avaliar a rede, ou seja, calcular a probabilidade condicional associada a cada nodo, dadas as evidências observadas até o momento. No caso geral, este é um problema NP-difícil mas, com o uso de heurísticas apropriadas, e dependendo do problema tratado, redes contendo milhares de nodos podem ser avaliadas em tempo aceitável [Cooper, 1987] [Charniak, 1991].

3.4 Raciocínio Baseado em Modelos

Raciocínio baseado em modelos (Model-Based Reasoning – MBR) é um paradigma da área de inteligência artificial que tem diversas aplicações na correlação de alarmes. Os

princípios de MBR foram originalmente propostos em [Davis *et al.*, 1982]. MBR consiste em se representar um sistema através de um modelo estrutural e de um modelo funcional, em contraste com os sistemas RB tradicionais, onde as regras se baseiam em associações empíricas. No caso de um sistema de gerência de redes de telecomunicações, a representação estrutural inclui a descrição dos elementos de rede e da topologia (i.e., conectividade e relações de inclusão – "containment"). A representação do comportamento funcional descreve os processos de propagação e de correlação de eventos [Jakobson e Weissman, 1995].

3.5 Quadro-negro

Diversos sistemas especialistas para gerência de redes e, particularmente, para correlação de alarmes, têm sido implementados utilizando uma arquitetura denominada quadro-negro ("blackboard") [Goyal e Worrest, 1988] [Sasisekharan *et al.*, 1993b] [Frontini *et al.*, 1991]. A arquitetura consiste de um banco de dados global, denominado *quadro-negro*, diversas *fontes de conhecimento* ("knowledge sources" — KS) e um *mecanismo de agenda* ("scheduler").

O quadro-negro [Shapiro *et al.*, 1987] é responsável por armazenar *elementos de solução* ("solution elements") produzidos pelo sistema durante o processo de resolução do problema. Os *elementos de solução* são organizados no quadro-negro segundo dois eixos, representando *níveis de abstração* e *intervalos de solução*, respectivamente.

Fontes de conhecimento são processos responsáveis por gerar *elementos de solução* e armazená-los no quadro-negro. Cada KS é definida por uma *condição* e por uma *ação*. A condição especifica em que situações a KS estará apta a contribuir na solução do problema, através de uma ação; normalmente caracteriza-se por uma dada configuração do quadro-negro. Geralmente, um dos efeitos de uma ação consiste na modificação do conteúdo do quadro-negro. As fontes de conhecimento são independentes entre si, ou seja, uma KS não pode invocar outras KSs, nem tem conhecimento sobre a funcionalidade, ou mesmo a existência dessas KSs.

Cada mudança no conteúdo do quadro-negro constitui um evento, capaz de ativar uma ou mais KS, dependendo das informações armazenadas no quadro-negro. O mecanismo de agenda é responsável, entre outras coisas, por selecionar, dentre as KS que tiveram sua condição satisfeita, quais as que serão disparadas. Através do uso de heurísticas *oportunistas*, o mecanismo de agenda pode escolher, em cada ciclo, qual a ação potencial mais adequada para a situação presente.

A arquitetura em quadro-negro contempla, entre outros, os seguintes objetivos [Shapiro *et al.*, 1987]: redução do espaço de pesquisa, através do raciocínio em múltiplos níveis de abstração, do uso de KS independentes e de agendamento oportunista; integração de diferentes tipos de conhecimento; operação simultânea de KSs redundantes, como estratégia para compensar a falta de confiabilidade do conhecimento disponível; independência entre os trabalhos das equipes de desenvolvimento de KSs; facilidade de modificação e de evolução.

3.6 Filtragem

Alguns sistemas de gerência de redes dispõem de filtros que selecionam as notificações de alarmes a serem exibidas, a pedido do operador, segundo critérios tais como área geográfica onde o alarme foi originado, área técnica (i.e., transmissão, comutação, etc.) ou grau de severidade do alarme. Nesses sistemas, o conceito de filtro é similar à definição do ITU-T [ITU-T, 1991]; os critérios de filtragem independem do contexto e baseiam-se exclusivamente nas características do próprio alarme [Meira, 1995]. Apesar de conseguirem reduzir bastante a quantidade de informações exibidas, os critérios de corte desses

filtros às vezes não contribuem para facilitar a identificação das falhas que causaram a emissão das notificações de alarme, podendo até mesmo impedir a apresentação de informações necessárias à identificação dessas falhas.

Existe uma modalidade de correlação alarmes, que poderia ser chamada *filtragem inteligente*, na qual o critério de seleção é mais elaborado, sendo calculado dinamicamente pelo sistema, em função de informações obtidas externamente ao alarme sendo filtrado [Möller *et al.*, 1995]. Esta técnica é apropriada para lidar com uma situação conhecida como "tempestade de eventos" [Hewlett Packard, 1995], na qual são gerados, em curto espaço de tempo, centenas ou até milhares de eventos, a partir de um único problema. Este fenômeno ocorre com freqüência em sistemas que usam tecnologias de alta velocidade, e.g., ATM (Asynchronous Transfer Mode) e SDH (Synchronous Digital Hierarchy) e precisa ser minimizado através de correlação de alarmes.

3.7 "Event Forwarding Discriminator" — EFD

Na Recomendação X.734 o ITU-T define os serviços, os protocolos e as unidades funcionais de um sistema de gerência no que se refere à função *relatório de eventos* ("event report") [ITU-T, 1993]. No modelo recomendado, antes de serem transferidas para fora de um objeto gerenciado, sob a forma de relatórios de eventos, as notificações localmente geradas são pré-processadas, dando origem a *relatórios de eventos em potencial*.

Um *Discriminador de Eventos a serem Transmitidos* ("Event Forwarding Discriminator" – EFD), tal como definido na Recomendação X.734, determina quais os *relatórios de eventos em potencial* devem ser transferidos, sob a forma de *relatórios de eventos*, para um destino e durante o intervalo de tempo especificados.

As condições a serem satisfeitas para que um relatório de evento em potencial possa ser transferido são especificadas através de um atributo denominado *discriminator construct*, que atua como um mecanismo de filtragem sobre os objetos apresentados à entrada do EFD. Os seguintes atributos de um objeto gerenciado podem ser especificados em um *discriminator construct* para serem avaliados por um EFD:

- Classe de objeto gerenciado;
- Instância de objeto gerenciado;
- Tipo de evento;
- Atributos de um dado tipo de evento, como, por exemplo, severidade.

Um EFD é um objeto gerenciado e, portanto, pode ser criado e destruído, além de poder ter o seu estado e os valores de seus atributos modificados a qualquer tempo.

3.8 Raciocínio Baseado em Casos

Como alternativa à abordagem baseada em regras, alguns autores propõem uma técnica denominada raciocínio baseado em casos ("case-based reasoning" – CBR) [Slade, 1991] [Weiner *et al.*, 1995]. Aqui, a unidade básica de conhecimento é um *caso*, e não uma *regra*. Casos consistem de registros contendo os aspectos mais relevantes de episódios passados; são armazenados, recuperados, adaptados e utilizados na solução de novos problemas. A experiência ganha com a solução destes novos problemas constitui novos casos, que são acrescèntados ao banco de dados, para uso futuro. Desta forma, o sistema é capaz de adquirir conhecimento por seus próprios meios, sem a necessidade de se entrevistar especialistas humanos. Outra característica marcante de sistemas CBR é a capacidade de modificar seu comportamento futuro em função dos erros cometidos. Além disto, um

sistema baseado em casos pode construir soluções para problemas inéditos, através da adaptação de casos passados à nova situação.

O desenvolvimento de sistemas CBR teve início na década de 1980 e, desde então, vários desafios têm estimulado a criatividade dos pesquisadores: como representar os casos; como indexá-los, de forma a permitir sua recuperação quando necessário; como modificar um caso antigo, para adaptá-lo a uma nova situação e gerar uma solução original; como testar a solução proposta, classificando-a como sucesso ou fracasso; como explicar a falha de uma solução sugerida e repará-la, dando origem a uma nova proposta.

O problema de adaptação de casos foi estudado por [Lewis e Dreo, 1993], que descrevem uma técnica denominada *adaptação parametrizada*, que se baseia na existência, em um bilhete de anormalidade, de certa relação entre as variáveis que descrevem um problema e as variáveis que especificam a correspondente solução. O sistema CBR leva em conta os parâmetros desta relação na proposição de uma solução para o caso que está sendo analisado. Para a representação dos parâmetros é proposto o uso de *variáveis linguísticas* (i.e., que assumem valores linguísticos, ao invés de valores numéricos) e o provimento de funções que traduzem os valores numéricos dos parâmetros em graus de pertinência a um conjunto nebuloso (cf. item 3.2).

Para armazenamento e recuperação de conhecimento sobre a solução de problemas passados, [Dreo e Valta, 1995] apresentam o conceito de *master ticket* que, ao invés de conter informações sobre uma única falha (caso), contém uma generalização das informações sobre a falha. Assim, ao se recuperar um *master ticket*, ele deve ser instanciado antes que a informação que contém possa ser aplicada a um caso particular. O objetivo é facilitar o acesso às informações sobre a solução de problemas. A generalização consiste em substituir por parâmetros todas as informações específicas da falha que originou o bilhete, tais como informações do usuário e endereços dos nodos envolvidos. Instanciar um *master ticket* consiste em substituir seus parâmetros pelos valores reais do caso que estiver sendo considerado.

3.9 Correlação por Codificação

Na abordagem de codificação ("coding approach") [Yemini *et al.*, 1996] [System Management ARTS, 1996] [Kliger *et al.*, 1995] a maior parte do processamento necessário à correlação dos alarmes é realizada previamente, dando origem a uma base de dados denominada *livro de código* ("codebook"). O livro de código pode ser visto como uma matriz, onde cada linha corresponde a um sintoma (ou evento, ou alarme) e cada coluna corresponde a um problema (ou falha, ou defeito). Se n sintomas distintos são representados no livro de código, cada elemento do vetor $p_i = (s_1, s_2, \ldots, s_n)$ contém a medida de causalidade do problema p_i em relação ao sintoma correspondente. Assim, se no vetor p_i, $s_1 = 0$, o sintoma s_1 nunca deverá ocorrer como conseqüência do problema p_i; por outro lado, se $s_1 = 1$, o sintoma s_1 sempre deverá ocorrer como conseqüência do problema p_i.

Não é exigido que os valores das medidas de causalidade pertençam ao conjunto $(0, 1)$; o modelo admite que estes valores pertençam a qualquer *semi-anel*, que constitui uma classe especial de conjuntos parcialmente ordenados. Isto deixa aberta a possibilidade do uso de diversas abordagens para a descrição da verossimilhança (*"likelihood"*) da causalidade, tais como modelos determinísticos, probabilísticos, fuzzy logic e modelos temporais [Lirov, 1993] [Luna e Corrêa Filho, 1992].

Em tempo real, cada situação de anormalidade pode ser descrita através de um vetor de alarmes $\underline{a} = (a_1, a_2, \ldots, a_n)$, onde cada elemento indica a ocorrência ou não do alarme correspondente. A correlação é feita através da escolha, no livro de código, do problema p cujo código mais se aproxima de $\underline{a}$, em termos de distância de Hamming [Tanenbaum, 1996].

Como a maior parcela da computação é realizada antecipadamente, apenas as operações mais simples são feitas em tempo real. Isto permite que o desempenho do "coding approach", em termos de eventos processados por segundo, possa ser de duas a quatro ordens de grandeza maior do que o desempenho de outras abordagens de correlação de alarmes encontradas na literatura [Yemini *et al.*, 1996] [Nygate, 1995] [Jakobson e Weissman, 1993].

O paradigma da orientação a objetos é adotado na abordagem de codificação para representar as classes de objetos da rede modelada, bem como seus atributos, relacionamentos e informações de eventos. Uma classe é um gabarito ("template") para um conjunto de instâncias de objetos, no qual são descritas as propriedades comuns a estes objetos, no que se refere à estrutura e ao comportamento.

Uma das principais motivações para o uso de orientação a objetos é permitir a interoperabilidade entre um sistema de correlação de alarmes e outras aplicações, executando em ambientes distribuídos heterogêneos. Para haver interoperabilidade entre duas aplicações é necessário que elas obedeçam aos mesmos padrões de interface, tais como, por exemplo, os definidos em [OMG e X/Open, 1995].

Os pontos fortes da abordagem do livro de códigos são: desempenho, robustez, computação automática das regras de correlação e versatilidade na adaptação do sistema a mudanças ocorridas na topologia da rede [Yemini *et al.*, 1996].

3.10 Localização Explícita

A maioria dos alarmes recebidos em um centro de gerência de rede não traz qualquer informação explícita sobre a localização da falha que lhes deu origem. Na proposta apresentada em [Bouloutas *et al.*, 1994], a cada alarme é explicitamente associada uma informação sobre localizações de falhas, consistindo de um conjunto que contém *todas* as localizações possíveis. Inicialmente é suposto que os alarmes sejam confiáveis e que haja apenas uma falha na rede. Desta forma, a falha se localizará na interseção dos conjuntos de localizações indicados pelos diversos alarmes. Em seguida, este cenário é estendido para cobrir múltiplas falhas, em um ambiente mais realístico onde os alarmes recebidos até podem não ser confiáveis. O problema inicial evolui para um problema de otimização discreta, onde o objetivo é descobrir o conjunto de falhas e o conjunto de alarmes que minimizam uma certa função de custo. Sendo este um problema NP-difícil, sua solução envolve o uso de heurísticas.

3.11 Correlação por Votação

Correlação por votação é uma técnica conceitualmente similar à técnica de localização explícita (cf. item 3.10). A principal diferença é que, ao invés de conter informações sobre a exata localização da falha — dadas por um conjunto contendo todas as possíveis localizações — como acontece na localização explícita, na correlação por votação cada alarme contém um número inteiro de *votos*, apontando a *direção* (em relação ao elemento que reporta o alarme) na qual pode estar o problema que o causou [Houck *et al.*, 1995].

Segundo esta técnica, um alarme não contém votos para cada nodo individual, mas para todos os nodos de uma dada direção. Portanto, é necessário que o sistema de correlação conheça a topologia da rede gerenciada para que, ao saber o número de votos de um alarme para uma dada direção, cada um dos nodos daquela direção receba aquele número de votos. Em seguida é possível fazer uma totalização dos votos de cada nodo, seguida da escolha daqueles nodos mais votados como possíveis localizações da falha.

A técnica de correlação por votação pode ser associada a outras técnicas como, por exemplo, pesquisa em árvores de dependência [Houck *et al.*, 1995], que permitam identificar, dentre os componentes dos nodos mais votados, qual aquele que mais provavelmente

é o responsável pela falha que causou os alarmes. Através desta pesquisa pode também ser determinado se a falha é imputável aos nodos identificados, ou se esses nodos falharam devido a um problema em componentes dos quais eles são dependentes.

3.12 Correlação "Proativa"

Nem sempre deve ser visto negativamente o fato de a rede gerenciada gerar um grande volume de alarmes, quando em situação de falha. É sabido que o processamento *manual* dessa massa de dados tende a tornar-se inviável à medida que aumenta a quantidade sistemas de alta velocidade na rede. As técnicas mais comuns de correlação de alarmes procuram trabalhar, em tempo real, diretamente sobre o fluxo de alarmes oriundo da planta, buscando eliminar a maioria deles, ou pelo menos "escondê-los" dos operadores e gerentes da rede, facilitando assim a identificação de falhas que *já ocorreram*.

Através das técnicas de garimpagem de dados ("data mining") e de descobrimento de conhecimento ("knowledge discovery") [Sasisekharan *et al.*, 1996] [Hätönen *et al.*, 1996], é possível descobrir padrões que caracterizam o comportamento atual e as tendências de comportamento futuro da rede. A técnica consiste em se varrer os dados disponíveis, sistematica e exaustivamente, aplicando técnicas de correlação e de aprendizado [Sasisekharan *et al.*, 1994].

Desta forma, é possível identificar problemas em potencial antes que eles se materializem, o que permite a manutenção "proativa" da rede [Sasisekharan *et al.*, 1993a].

A abordagem consiste em examinar o comportamento dos elementos da rede ao longo do tempo, considerando padrões de comportamento comuns a elementos da mesma classe. Tendo um forte componente empírico (representado pelos dados coletados), a abordagem também inclui conhecimento sobre os elementos e a topologia da rede. A computação pode ser dividida em três passos:

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 do problema e solucioná-lo.

A necessidade de envolvimento humano no processo de identificação de falhas é enfatizado por [Sasisekharan *et al.*, 1996], devido ao fato de que o problema não se encontra ainda completamente resolvido.

3.13 Correlação Distribuída

Com o crescimento das redes de telecomunicações, tanto em tamanho quanto em complexidade, pode ser recomendável o particionamento do ambiente de gerência em um certo número de domínios de gerência, para que sejam alcançados os requisitos de qualidade desejados na operação e manutenção do sistema. Um exemplo desta arquitetura organizacional pode ser encontrado em [Nogueira e Meira, 1996].

A adoção de uma arquitetura distribuída para o sistema de gerência de rede facilita a implementação de esquemas de localização distribuída de falhas e justifica o desenvolvimento de algoritmos distribuídos para essa localização.

[Katzela *et al.*, 1995] apresentam um modelo da rede de telecomunicações gerenciada no qual é assumida a abordagem de gerência distribuída. A rede é particionada em diversos domínios estáticos, disjuntos e logicamente autônomos, cada um deles gerenciado por um único centro de gerência. Cada centro de gerência tem uma visão limitada do estado dos demais domínios. Entretanto, gerentes de diferentes domínios comunicam-se entre si e trocam informações sobre o estado de seus domínios. Como os alarmes gerados

em conseqüência de uma determinada falha podem não se restringir a um único domínio, os centros de gerência têm que colaborar no sentido de inferir o estado real do sistema. É assumido que os processos de transferência de informações entre gerentes e as demais partes da TMN *não* são afetados por falhas.

No modelo apresentado, o conjunto dos objetos gerenciados cuja falha pode causar um determinado alarme é definido como o *domínio do alarme*. Antes de iniciar o processo de localização da falha, o centro de gerência deve descobrir o domínio de cada um dos alarmes recebidos — o que pode ser feito através de *localização explícita* [Bouloutas *et al.*, 1994] (cf. item 3.10). Um *agrupamento* ("cluster") de alarmes é um conjunto de alarmes cujos domínios têm uma interseção diferente de $\emptyset$ (conjunto vazio).

Cada agrupamento de alarmes pode ter uma ou mais causas possíveis. O algoritmo de localização de falhas deve descobrir a "melhor" (ou seja, a mais provável) dentre estas causas possíveis. Isto poderia ser feito a partir da atribuição de uma probabilidade de falha a cada objeto gerenciado. A partir daí, a "melhor" causa para o agrupamento de alarmes poderia ser definida como sendo o conjunto de objetos gerenciados cuja probabilidade de falha combinada fosse máxima. Ao invés de se atribuir uma probabilidade de falha a cada objeto gerenciado, [Katzela *et al.*, 1995] associa a cada um desses objetos um "*custo de informação*", definido como o logaritmo negativo da probabilidade de falha do objeto. Então, a "melhor" causa, ou seja, a mais provável, será dada pelo conjunto de objetos gerenciados cuja soma de custos de informação é mínimo.

Como a localização de falhas é um problema NP-Completo, no caso geral não há algoritmo polinomial que dê uma solução exata para o problema. Entretanto, sendo dados um agrupamento de alarmes recebidos (A) e o conjunto de objetos gerenciados associado a A, pode ser demonstrado que existe um algoritmo polinomial que acha uma solução exata se o número máximo de falhas simultâneas for menor que um parâmetro k. Portanto, pode ser assumido que existe um algoritmo centralizado que descobre as falhas mais prováveis em um conjunto de objetos gerenciados, dado um conjunto de alarmes e os custos de informação associados a cada objeto gerenciado [Katzela *et al.*, 1996]. Q, a probabilidade de haver mais de k falhas simultâneas no sistema, é também a probabilidade de o algoritmo não fornecer uma solução para o problema.

Com relação à distribuição do processo de correlação, são identificadas três abordagens para localização de falhas:

1. Localização centralizada. Assume a existência de um gerente central, que tem uma visão global da rede e cuja área de atuação inclui os domínios de todos os demais gerentes. O gerente central resolve diretamente qualquer problema que afeta mais de um domínio de gerência.

2. Localização descentralizada. Neste caso, os problemas que afetam mais de um domínio são resolvidos através de uma colaboração entre o gerente central e os gerentes dos domínios afetados.

   Cada gerente de domínio é responsável por calcular as soluções parciais para o problema, contendo as possíveis causas dos alarmes cujos *domínios* incluam objetos de mais de um *domínio de gerência*, e enviá-las ao gerente central, que deverá descobrir, dentre estas soluções parciais, quais são as soluções *compatíveis*. Duas soluções parciais são compatíveis se todos os alarmes recebidos por todos os gerentes de domínio são explicados pela solução final.

   Finalmente, o gerente central seleciona a solução global compatível que tenha o mínimo custo de informação.

3. Localização distribuída. Esta abordagem consiste em tentar descobrir as causas dos alarmes sem a interveniência de um gerente central.

Seja a rede de telecomunicações dividida em dois domínios, 1 e 2. Do ponto de vista do gerente do domínio 1, para cada alarme cujo domínio cruza a fronteira, seria desejável associar-se a probabilidade de que ele seja explicado pelo domínio 2. Para isto, todos os objetos gerenciados que pertencem ao domínio 2 e estejam associados com o alarme são associados a um "nodo procurador" ("proxy node"). A falha de um nodo procurador indica que um ou mais objetos do domínio 2 falhou.

Pode ser demonstrado que o cálculo da probabilidade de falha de um nodo procurador é um problema NP-completo. O melhor que pode ser feito é uma estimativa desta probabilidade, o que introduz um erro, que por sua vez impede que se possa garantir uma solução global ótima [Katzela *et al.*, 1996].

3.14 Redes Neuroniais Artificiais

Uma rede neuronial artificial (ANN) é um sistema constituído de elementos ("*neurônios*") interconectados segundo um modelo que procura reproduzir a rede neuronial existente no cérebro humano. Conceitualmente, cada *neurônio* pode ser considerado como uma unidade de processamento autônoma, dotada de memória local e de canais unidirecionais de comunicação com outros neurônios. O funcionamento de um canal de entrada em uma ANN inspira-se no funcionamento de um *dendrito* nos neurônios biológicos; de maneira análoga, um canal de saída tem como padrão um *axônio*. Um neurônio possui apenas um axônio, mas pode possuir um número arbitrário de dendritos (em um neurônio biológico existem da ordem de dez mil). O "sinal" de saída de um neurônio pode ser utilizado como entrada para um número arbitrário de neurônios [Meech e Kumar, 1994] [Mead, 1989].

Na sua forma mais simples, o processamento realizado em um neurônio consiste em efetuar a soma ponderada dos sinais presentes em suas entradas e gerar um sinal de saída se o resultado da soma ultrapassar um certo limite ("*limiar*"). No caso mais geral, o processamento pode incluir qualquer tipo operação matemática sobre os sinais de entrada, levando-se também em consideração os valores armazenados na memória local do neurônio [Meira Júnior, 1993].

Uma das principais motivações para o desenvolvimento das ANN é a utilização de computadores para tratar de uma classe de problemas que são facilmente resolvidos pelo cérebro humano, mas que não conseguem ser tratados com eficácia com a utilização exclusiva dos paradigmas de programação convencionais.

Devido à frustração da grande expectativa que se avolumou a partir das primeiras pesquisas sobre modelagem do sistema nervoso, nos anos quarenta, o interesse pelas ANNs reduziu-se sensivelmente ao final da década de sessenta, quando estudos teóricos revelaram fortes limitações desse paradigma [Michalski *et al.*, 1983]. O interesse pela área renasceu a partir do início dos anos oitenta, quando o desempenho dos computadores passou a permitir implementações práticas, as quais têm um alto custo computacional. Também contribuiu para este "renascimento" o descobrimento de novas aplicações para as ANNs.

Controle e armazenamento distribuído de dados e paralelismo são características marcantes das ANN; além disso, uma ANN não requer conhecimento prévio do relacionamento matemático entre entradas e saídas, que pode ser *aprendido* automaticamente, durante a operação normal do sistema. Isso as torna, a princípio, uma boa alternativa para aplicações — tais como correlação de alarmes e diagnóstico de falhas — onde as relações entre falhas e alarmes nem sempre são bem definidas ou compreendidas, e onde os dados disponíveis às vezes são ambíguos ou inconsistentes [Covo *et al.*, 1989].

Uma excelente introdução às redes neuroniais pode ser encontrada em [Meira Júnior, 1993].

4 Comparação Entre as Alternativas Disponíveis

A comparação entre os métodos e algoritmos apresentados na Seção 3 é um processo difícil e deve levar em consideração os seguintes fatores, entre os quais, em geral, existe uma relação de compromisso: (1) facilidade de modelagem teórica da *rede objeto*, i.e., a rede que irá gerar os alarmes a serem correlacionados; (2) facilidade de implementação; (3) facilidade de adaptação a mudanças na rede objeto; (4) desempenho; (5) precisão. Embora seja possível, em princípio, quantificar esses fatores no caso de uma rede objeto específica, é difícil imaginar como isso poderia ser feito para uma rede objeto genérica. Dificuldade semelhante existe quando se procura comparar diferentes estratégias sem se especificar a *aplicação* a que se destina a correlação (por exemplo: redução da quantidade de informação a ser analisada pelo operador; identificação das falhas que deram origem aos alarmes; previsão quanto à ocorrência de falhas no futuro). Portanto, uma comparação entre abordagens para correlação de alarmes deve levar em conta tanto a aplicação a que se destina, quanto as características da rede objeto — ou, no mínimo, a *classe de redes objetos*: SDH, ATM, comutação SPC, etc.

Em geral, abordagens baseadas em regras são indicadas para correlação em elementos de redes, ou em redes cuja configuração raramente se altera; os altos custos de implementação e de adaptação a mudanças na rede objeto dificultam a aplicação dessas estratégias em grandes redes de telecomunicações. Outras abordagens, tais como aquelas baseadas em casos, são menos sensíveis a mudanças na rede objeto, mas ainda carecem de um embasamento teórico que permita a sua utilização em redes comerciais de grande porte (cf. item 3.8).

Portanto, não existe uma solução única que seja a "melhor", em termos de precisão e/ou de complexidade, para resolver um problema genérico de correlação de alarmes. A opção a ser adotada em um caso específico deve ser escolhida tendo em vista as virtudes e as limitações das diversas abordagens aplicáveis àquele caso. Um levantamento das principais soluções, produtos e plataformas de correlação de alarmes encontrados no mercado pode ser encontrada em [Meira, 1996].

5 Conclusões

Neste trabalho foram reunidos e organizados alguns dos principais conceitos necessários ao estudo de correlação de alarmes.

Diversas soluções têm sido propostas para correlação de alarmes em redes de telecomunicações. A maioria dessas propostas consiste de variações sobre a clássica abordagem baseada em regras. Neste caso se incluem as propostas baseadas em lógica difusa, as baseadas em modelos ou aquelas baseadas em "quadro-negro", por exemplo. Outros trabalhos baseiam-se em visões completamente diferentes do problema de correlação, representando novas frentes de pesquisa. Neste último caso podem ser citadas as abordagens baseadas em casos, a correlação por codificação e as redes neuroniais. As mais importantes dentre essas abordagens foram identificadas neste trabalho, que procurou também ressaltar os pontos fortes e os pontos fracos de cada uma delas.

Referências

[Bouloutas *et al.*, 1994] A. T. Bouloutas, S. Calo, e A. Finkel. Alarm correlation and fault identification in communication networks. *IEEE Transactions on Communications*, 42(2/3/4):523–533, Feb/Mar/Apr 1994.

[Brownston *et al.*, 1986] Lee Brownston, Robert Farrel, Elaine Kant, e Nancy Martin. *Programming Expert Systems in OPS5: An Introduction to Rule-Based Programming.* Addison-Wesley, 1986.

[Charniak e McDermott, 1986] Eugene Charniak e Drew McDermott. *Introduction to Artificial Intelligence.* Addison-Wesley, Reading, USA, 1986.

[Charniak, 1991] Eugene Charniak. Bayesian networks without tears. *AI Magazine*, (Winter 1991):50–63, 1991.

[Chen e Rao, 1993] Jian-Liang Chen e Nutakki D. Rao. A fuzzy expert system for fault diagnosis in electric distribution systems. In *Canadian Conference on Electrical and Computer Engineering - CCECE'93*, p. 1283–6 v. 2, Vancouver, Canada, 1993. IEEE.

[Cooper, 1987] G. F. Cooper. Probabilistic inference using belief networks is NP-Hard. Rel. Téc. KSL-87-27, Medical Computer Science Group, Stanford University, 1987.

[Covo *et al.*, 1989] A.A. Covo, T.M. Moruzzi, e E.D. Peterson. AI-assisted telecommunications network management. In *IEEE Global Telecommunications Conference (GLOBECOM 89)*, páginas 487–491, Dallas, TX, USA, Nov 1989.

[Cronk *et al.*, 1988] R. Cronk, P. Callahan, e L. Bernstein. Rule-based expert systems for network management and operations. *IEEE Network*, 2(5):7–21, 1988.

[Davis *et al.*, 1982] R. Davis, H. Shrobe, W. Hamscher, K. Wieckert, M. Shirley, e S. Polit. Diagnosis based on description of structure and functions. In *National Conference on Artificial Intelligence*, páginas 137–142, Pittsburg, PA, 1982.

[Deng *et al.*, 1993] Robert H. Deng, Aurel A. Lazar, e Weiguo Wang. A probabilistic approach to fault diagnosis in linear lightwave networks. In *IFIP International Symposium on Integrated Network Management, III (ISINM'93)* [1993], páginas 697–708.

[DeSalvo, 1988] Daniel A. DeSalvo. *Knowledge Acquisition for Knowledge-Based Systems*, páginas 267–303. In Liebowitz [1988], 1988.

[Dreo e Valta, 1995] Gabi Dreo e Robert Valta. Using master tickets as a storage for problem-solving expertise. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 328–340.

[Frontini *et al.*, 1991] M. Frontini, J. Griffin, e S. Towers. A knowledge-based system for fault localization in wide area networks. In *IFIP International Symposium on Integrated Network Management, II* [1991], páginas 519–530.

[Gering, 1993] Michael Gering. CMIP versus SNMP. In *IFIP International Symposium on Integrated Network Management, III (ISINM'93)* [1993], páginas 347–359.

[Ginsberg, 1993] Matt Ginsberg. *Essentials of Artificial Intelligence.* Morgan Kaufman, San Francisco, USA, 1993.

[GLO, 1993] *IEEE Global Telecommunications Conference (GLOBECOM 93)*, Huston, TX, USA, Nov 1993.

[Goodman *et al.*, 1993] Rodney M. Goodman, Barry Ambrose, Hayes Latin, e Sandee Finnell. A hybrid expert system / neural network traffic advice system. In *IFIP International Symp.on Integr. Network Management, III (ISINM'93)* [1993], p. 607–16.

[Goodman e Latin, 1991] Rodney M. Goodman e Hayes Latin. Automated knowledge acquisition from network management databases. In *IFIP International Symposium on Integrated Network Management, II* [1991], páginas 541–549.

[Goyal e Worrest, 1988] Shri K. Goyal e Ralph W. Worrest. *Expert System Applications to Network Management*, páginas 3–44. In Liebowitz [1988], 1988.

[Gupta *et al.*, 1985] Madan M. Gupta, A. Kandel, W. Bandler, e Jerzy B. Kiszka, ed. *Approximate Reasoning in Expert Systems*. North-Holland, Amsterdam, 1985.

[Hall, 1987] N. Green Hall. *A Fuzzy Decision Support System for Strategic Planning*, páginas 77–90. In Sanchez e Zadeh [1987], 1987.

[Hätönen *et al.*, 1996] Kimmo Hätönen, Mika Klemettinen, Heikki Mannila, Pirjo Ronkainen, e Hannu Toivonen. TASA: Telecommunication Alarm Sequence Analyzer or How to enjoy faults in your network. In *IEEE/IFIP 1996 Network Operations and Management Symposium (NOMS'96)* [1996], p. 520–9.

[Henkind *et al.*, 1987] S.J. Henkind, R.R. Yager, A.M. Benis, e M.C. Harrison. *A Clinical Alarm System Using Techniques from Artificial Intelligence and Fuzzy Set Theory*, páginas 91–104. In Sanchez e Zadeh [1987], 1987.

[Henrion *et al.*, 1991] Max Henrion, John S. Breese, e Eric J. Horvitz. Decision analysis and expert systems. *AI Magazine*, (Winter 1991):64–91, 1991.

[Hewlett Packard, 1995] Hewlett Packard. HP OpenView event correlation for the telecommunications environment: Technology brief, September 1995.

[Houck *et al.*, 1995] K. Houck, S. Calo, e A. Finkel. Towards a practical alarm correlation system. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 226–237.

[ICC, 1993] *IEEE International Conference on Communications'93 (ICC 93)*, 1993.

[ISI, 1991] *IFIP International Symposium on Integrated Network Management, II*. Elsevier Science (North-Holland), 1991.

[ISI, 1993] *IFIP International Symposium on Integrated Network Management, III (ISINM'93)*, San Francisco, CA, USA, 1993.

[ISI, 1995] *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)*, Santa Barbara, CA, USA, 1995. Chapman & Hall.

[ITU-T, 1991] ITU-T. Recommendation X.710: Common Management Information Service definition for CCITT applications, 1991.

[ITU-T, 1992a] ITU-T. Recommendation M.3010: Principles for a Telecommunications Management Network, October 1992.

[ITU-T, 1992b] ITU-T. Recommendation X.700: Management framework for Open Systems Interconnection (OSI) for CCITT applications, September 1992.

[ITU-T, 1992c] ITU-T. Rec.X.720: Open Systems Interconnection - structure of management information: Management information model, January 1992.

[ITU-T, 1992d] ITU-T. Recommendation X.733: Information technology - Open Systems Interconnection - systems management: Alarm reporting function, 1992.

[ITU-T, 1992e] ITU-T. Recommendation X.735: Information technology - Open Systems Interconnection - systems management: Log control function, September 1992.

[ITU-T, 1993] ITU-T. Recommendation X.734: Information technology - Open Systems Interconnection - systems management: Event report management function, 1993.

[ITU-T, 1995] ITU-T. Recommendation M.3010: Principles for a Telecommunications Management Network. Draft M.3010 version MÜN/950630/a, June 1995.

[Jakobson e Weissman, 1993] Gabriel Jakobson e Mark D. Weissman. Alarm correlation. *IEEE Network*, 7(6):52–59, November 1993.

[Jakobson e Weissman, 1995] G. Jakobson e M. Weissman. Real-time telecommunication network management: extending event correlation with temporal constraints. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], p. 290–301.

[Katzela *et al.*, 1995] I. Katzela, A.T. Bouloutas, e S.B. Calo. Centralized vs distributed fault localization. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 250–261.

[Katzela *et al.*, 1996] I. Katzela, A.T. Bouloutas, e S. Calo. Comparison of distributed fault identification schemes in communication networks. Relatório técnico, IBM Corp., T.J. Watson Research Center, Yorktown Heights, NY, USA, January 1996.

[Katzela e Schwartz, 1995] I. Katzela e M. Schwartz. Schemes for fault identification in communication networks. *IEEE Trans. on Networking*, 3(6):753–64, Dec 1995.

[Kehl e Hopfmüller, 1993] Walter Kehl e Heinrich Hopfmüller. Model-based reasoning for the management of telecommunication networks. In *IEEE International Conference on Communications'93 (ICC 93)* [1993], páginas 13–17.

[Kirsch e Kroschel, 1994] H. Kirsch e K. Kroschel. Applying bayesian networks to fault diagnosis. In *3rd IEEE Conference on Control Applications*, p. 895–900. IEEE, 1994.

[Kliger *et al.*, 1995] S. Kliger, S. Yemini, Y. Yemini, D. Ohsie, e S. Stolfo. A coding approach to event correlation. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 266–277.

[Lebailly *et al.*, 1987] J. Lebailly, R. M.-Clouaire, e H. Prade. *Use of Fuzzy Logic in a Rule-Based System in Petroleum Geology*, p. 125–44. In Sanchez e Zadeh [1987], 1987.

[Lewis e Dreo, 1993] Lundy Lewis e Gabi Dreo. Extending trouble ticket systems to fault diagnostics. *IEEE Network*, 7(6):44–51, November 1993.

[Lewis, 1993] Lundy Lewis. A case-based reasoning approach to the resolution of faults in communications networks. In *IFIP International Symposium on Integrated Network Management, III (ISINM'93)* [1993], páginas 671–682.

[Liebowitz, 1988] J. Liebowitz, editor. *Expert System Applications to Telecommunications*. John Wiley and Sons, New York, NY, USA, 1988.

[Lirov, 1993] Yuval Lirov. Fuzzy logic for distributed systems troubleshooting. In *Fuzzy Systems International Conference 1993*, páginas 986–991. IEEE, 1993.

[Luna e Corrêa Filho, 1992] Henrique P. L. Luna e Milton Corrêa Filho. A probabilistic and informational basis to optimize expert systems. *Investigación Operativa*, 2(3):273–296, Junio 1992.

[Luna, 1994] Henrique Pacca L. Luna. Sistemas de apoio à decisão, 1994. Departamento de Ciência da Computação da UFMG.

[Mansfield *et al.*, 1993] G. Mansfield, K. Jayanthi, K. Higuchi, Y. Nemoto, e S. Noguchi. The MIKB model for intelligent network management. In *IEEE International Conference on Communications'93 (ICC 93)* [1993], páginas 1210–1214.

[Mead, 1989] Carver Mead. *Analog VLSI and Neural Systems.* Addison-Wesley, Reading, USA, 1989.

[Meech e Jordon, 1993] J.A. Meech e L.A. Jordon. Development of a self-tuning fuzzy logic controller. *Minerals Engineering*, 6(2):119–131, 1993.

[Meech e Kumar, 1994] John A. Meech e Sunil Kumar. *A Hypermanual on Expert Systems.* Canada Centre for Mineral and Energy Technology — CANMET, Ottawa, Canada, 3ª edição, 1994. Hypertext Book.

[Meira Júnior, 1993] Wagner Meira Júnior. Implementação de redes neuroniais em ambientes paralelos. Dissertação de Mestrado, UFMG, Belo Horizonte, Brasil, 1993.

[Meira, 1995] Dilmar M. Meira. Managing a telecommunication network with SIS. Relatório Técnico DCC 011/95, Department of Computer Science of the Federal University of Minas Gerais, Belo Horizonte, Brasil, 1995.

[Meira, 1996] Dilmar M. Meira. Um survey sobre correlação de alarmes. Relatório Técnico DCC, Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, Belo Horizonte, Brasil, Dezembro 1996.

[Michalski *et al.*, 1983] R.S. Michalski, J.G. Carbonell, e T.M. Mitchell, ed. *Machine Learning: An Artificial Intelligence Approach.* Springer-Verlag, Berlin, 1983.

[Möller *et al.*, 1995] M. Möller, S. Tretter, e B. Fink. Intelligent filtering in network management systems. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 304–315.

[Negoita, 1984] Constantin Virgil Negoita. *Expert Systems and Fuzzy Systems.* Benjamin/Cummings, Menlo Park, USA, 1984.

[Nilsson, 1980] Nils J. Nilsson. *Principles of artificial intelligence.* Tioga, Palo Alto, USA, 1980.

[Nogueira e Meira, 1996] José M. S. Nogueira e Dilmar M. Meira. The SIS project: A distributed platform for the integration of telecommunication management systems. In *IEEE/IFIP 1996 Network Operations and Management Symposium (NOMS'96)* [1996], páginas 175–185.

[NOM, 1996] *IEEE/IFIP 1996 Network Operations and Management Symposium (NOMS'96)*, Kyoto, Japan, April 1996.

[Nygate, 1995] Y. A. Nygate. Event correlation using rule and object based techniques. In *IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95)* [1995], páginas 278–289.

[OMG e X/Open, 1995] OMG e X/Open. The Common Object Request Broker: Architecture and specification, July 1995. Revision 2.0.

[Pearl, 1984] Judea Pearl. *Heuristics: Intelligent Search Strategies for Computer Problem Solving.* Addison-Wesley, Reading, USA, 1984.

[Pearl, 1991] Judea Pearl. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, USA, 1991. Rev. 2nd. Printing.

[Rich, 1983] Elaine Rich. *Artificial Intelligence*. McGraw-Hill, New York, USA, 1983.

[Sanchez e Zadeh, 1987] Elie Sanchez e Lofti Asker Zadeh, editores. *Approximate Reasoning in Intelligent Systems, Decision and Control*. Pergamon, England, 1987.

[Sasisekharan *et al.*, 1993a] R. Sasisekharan, V. Seshadri, e S.M. Weiss. Proactive network maintenance using machine learning. In *IEEE Global Telecommunications Conference (GLOBECOM 93)* [1993], páginas 217–222.

[Sasisekharan *et al.*, 1993b] Raguram Sasisekharan, Yung-Kao Hsu, e David Simen. SCOUT: An approach to automating diagnosis of faults in large scale networks. In *IEEE Global Telecommunications Conference (GLOBECOM 93)* [1993], p. 212–16.

[Sasisekharan *et al.*, 1994] Raguram Sasisekharan, V. Seshadri, e Sholom M. Weiss. Using machine learning to monitor network performance. In *IEEE Conference on Artificial Intelligence Applications*, páginas 92–98. IEEE, 1994.

[Sasisekharan *et al.*, 1996] Raguram Sasisekharan, V. Seshadri, e Sholom M. Weiss. Data mining and forecasting in large-scale telecommunication networks. *IEEE Expert*, 11(1):37–43, February 1996.

[Shapiro *et al.*, 1987] Stuart C. Shapiro, David Eckroth, e George A. Vallasi, editores. *Encyclopedia of Artificial Intelligence*, capítulo "Blackboard Systems", por B. Hayes-Roth, páginas 73–80. John Wiley & Sons, New York, USA, 1987.

[Slade, 1991] S. Slade. Case-based reasoning: A research paradigm. *AI Magazine*, 12(1):42–55, Spring 1991.

[Smets *et al.*, 1988] Philippe Smets, Abe Mamdani, Didier Dubois, e Henri Prade, ed. *Non-Standard Logics for Automated Reasoning*. Academic Press, England, 1988.

[Sutter e Zeldin, 1988] Mark T. Sutter e Paul E. Zeldin. Designing expert systems for real-time diagnosis of self-correcting networks. *IEEE Network*, p. 43–51, Sept 1988.

[System Management ARTS, 1996] System Management ARTS. InCharge data sheet, Setembro 1996. http://www.smarts.com/products/incharge_datasheet.html.

[Tanenbaum, 1996] Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall, Upper Saddle River, USA, 3ª edição, 1996.

[Veiga e Meech, 1994] M.M. Veiga e J.A. Meech. Application of fuzzy logic to environmental risk assessment. In *Meeting of the Southern Hemisphere on Mineral Technology, IV*, páginas 355–370, Concepción, Chile, 1994.

[Weiner *et al.*, 1995] Andrew J. Weiner, David A. Thurman, e Christine M. Mitchell. Applying case-based reasoning to aid fault management in supervisory control. In *Proceedings of the 1995 IEEE International Conference on Systems, Man and Cybernetics*, páginas 4213–4218, Vancouver, BC, Canada, 1995. IEEE.

[Yemini *et al.*, 1996] Shaula Alexander Yemini, Shmuel Kliger, Eyal Mozes, Yechiam Yemini, e David Ohsie. High speed and robust event correlation. *IEEE Communications Magazine*, páginas 82–90, May 1996.

[Zadeh, 1965] Lofti A. Zadeh. Fuzzy sets. *Information and Control*, 8:338–353, 1965.

[Zadeh, 1988] Lotfi A. Zadeh. Fuzzy logic. *Computer*, páginas 83–93, April 1988.