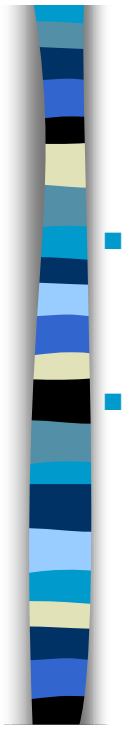
Correlação de alarmes

Motivação

- A melhoria na gerência da rede
  - **melhoria na qualidade dos serviços, do ponto de vista dos usuários;**
  - **aumento de receita, através de acréscimo do tráfego cursado na rede;**
  - **redução nos custos de operação e manutenção da rede.**

Gerência de falhas

- Engloba
  - **detecção,**
  - **isolação e**
  - **correção de falhas**
- Funções que só podem ser realizadas a partir da adição de valor aos dados brutos coletados da planta.



Excesso de informações

- **Para uma planta de telecomunicações típica o problema relacionado à carência de informações no centro de gerência de rede está gradativamente perdendo relevância.**
- **De fato, com o crescimento da planta gerenciada, associado à implantação de modelos de gerência, está havendo um grande aumento no volume de informações recebidas nos centros de gerência, tornando praticamente inviável o processamento "manual" de todas elas**

Correlação de alarmes

- Correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, resultando na atribuição de um novo significado aos alarmes originais
- Como parte do processo de correlação, dados brutos são interpretados e analisados, levando em consideração um conjunto de critérios pré-estabelecidos, ou definidos dinamicamente em função do processo de gerência.

Correlação de Alarmes em Redes de Telecomunicações

- **Em 1985, para permitir a implementação de redes de gerência a partir de equipamentos e sistemas multivendedores, o ITU- T iniciou a especificação de sua Rede de Gerência de Telecomunicações, mais conhecida como TMN**
- **TMN é o modelo geral de uma rede para dar suporte às necessidades de gerência de uma companhia de telecomunicações para planejar, prover, instalar, manter, operar e administrar redes e serviços de telecomunicações.**

OS

- Um sistema de suporte à operação ("Operations Support System" -OS) é um programa que processa informações relacionadas à gerência de telecomunicações, com o objetivo de monitorar, coordenar e/ou controlar as funções de telecomunicações.
- Um OS caracteriza-se por implementar funções de gerência denominadas OSFs ("Operations Systems Functions")

Elemento de rede

- Denomina-se elemento de rede um equipamento que se comunica com a TMN, segundo padrões definidos pelo ITU-T, com o propósito de ser monitorado e/ou controlado.

Objeto gerenciado

- Um objeto gerenciado é definido como uma visão de um recurso (rede de telecomunicações), sob o ponto de vista do sistema de gerência
- 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.

Relatórios de eventos

- Relatórios de eventos são utilizados para, através do uso de protocolos de comunicação, reportar a ocorrência de eventos em um objeto gerenciado.
- No contexto de gerência de redes, uma falha é definida como uma 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.

Alarme

- 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

Correlação de alarmes

- Processo no qual se cria um conjunto mínimo de hipóteses de falhas para um dado conjunto de alarmes
- Correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais

Objetivo da correlação de alarmes

- 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.

Aplicação da correlação de alarmes

- Correlação de alarmes pode ser aplicada a qualquer das cinco áreas funcionais de gerência
  - **falhas,**
  - **configuração,**
  - **contabilização,**
  - **desempenho e**
  - **segurança**

Gerenciamento em tempo real

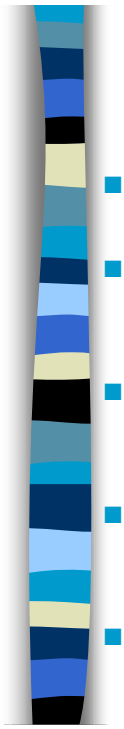
- O principal requisito para se fazer gerência de falhas de forma integrada é a disponibilização, em um centro de gerência, de informações sobre o funcionamento da rede, em tempo real

Processamento do alarme

- 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.

Processamento dos alarmes

- Muitas das notificações recebidas não contêm informação original.
- A ocorrência de uma única falha na rede supervisionada às vezes resulta no recebimento múltiplas notificações.
- Diversos fatores contribuem para esta situação

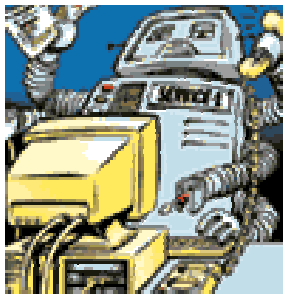


Excesso de alarmes

- 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.

Correlação = automação

- 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.



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.

Sistema de diagnóstico de falhas

- Um sistema para diagnóstico de falhas deve possuir um modelo da configuração gerenciada, que processe o fluxo de alarmes em tempo real e seja capaz de trabalhar com dados incompletos

Sistema de diagnóstico de falhas

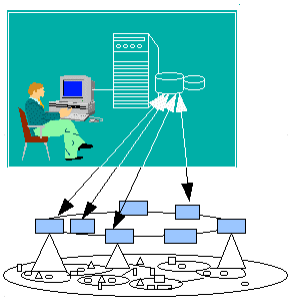
- Além disto, espera-se que ele seja capaz de identificar mudanças na aparência e na importância dos problemas em função do tempo (e.g., horário, dia da semana, estação do ano), de separar causa de efeitos e resolver os problemas por ordem de severidade (i.e., os problemas mais graves devem ter prioridade).

Testes

- 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

Interpretação

- É desejável que o sistema consiga, de alguma forma, interpretar os resultados dos testes



Barreiras

- 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.

Dados adicionais

- A correlação pode demandar outras informações, tais como resultados de testes executações na rede, dados obtidos em bancos de dados externos e junto aos usuários

Aspectos adicionais

- **Ruídos**, constituídos por informação insignificante, informação redundante, alarmes repetidos ("streaming alarms"), alarme transitório ("occasional spike"), alarme intermitente ("frequent oscilation") e ocorrência repetida;
- **Dependências Ocultas**. Muitas vezes a estratégia adotada na correlação exige a construção de um modelo da rede gerenciada.
- **Simplificações** adotadas nesse modelo podem tornar alguns elementos de rede gerenciada "invisíveis" ao processo de relação. Isto permite que uma falha ocorrida em um elemento de rede "invisíveis" simule a ocorrência de uma falha em um outro elemento de rede;

Aspectos adicionais

- **Dependências Complexas**. O modelo de dependências adotado muitas vezes pressupõe que, quando um recurso de suporte falha, todos os elementos que dependem deste recurso também falharão, o que às vezes não acontece;
- **Dados Incompletos**. Em geral se pressupõe que todas as informações necessárias à correlação são enviadas espontaneamente pelos elementos da rede. Às vezes algumas destas informações não são disponibilizadas (por exemplo, devido a uma interrpção em um enlace sem caminho alternativo).

Tipos de correlação

- Compressão
- Supressao seletiva
- Filtragem
- Contagem
- Escalação
- Generalização
- Especialização
- Relacionamento temporal
- Aglutinação

Compressão

- Compressão consiste em detectar, a partir da observação dos alarmes recebidos em uma dada "janela" de tempo, múltiplas ocorrências de um mesmo evento, substituindo os alarmes correspondentes por um único alarme, possivelmente indicando quantas vezes o evento ocorreu durante o período de observação.

Supressão Seletiva

- Supressão Seletiva é a inibição temporária dos alarmes referentes a um dado evento, segundo critérios - continuamente avaliados pelo sistema de correlação - relacionados ao contexto dinâmico do processo de gerência de rede.
- Os critérios de supressão geralmente estão vinculados à presença de outros alarmes, ao relacionamento temporal entre alarmes ou a prioridades estabelecidas pelos gerentes da rede.

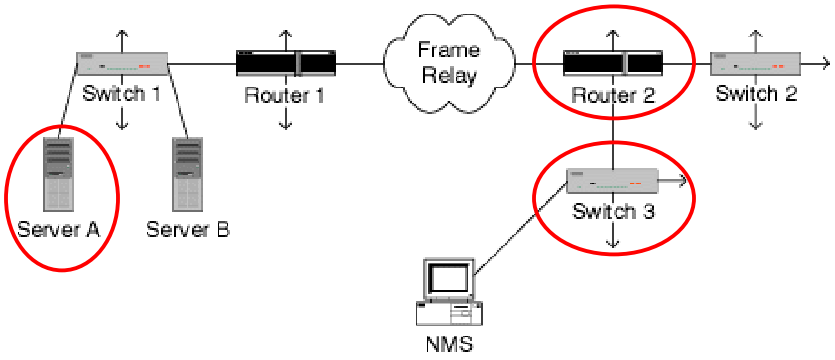
Filtragem

- Filtragem consiste em suprimir um determinado alarme, em função dos valores de um conjunto de parâmetros, previamente especificados.
- Em um sentido estrito, a filtragem leva em consideração apenas os parâmetros do alarme que estiver sendo filtrado.
- Em um sentido mais amplo, a filtragem pode levar em consideração quaisquer outros critérios.
- Nesse caso, que poderia ser caracterizado como uma filtragem inteligente, o conceito de filtragem se expande, podendo englobar diversos outros tipos de operações, tais como compressão e supressão.

Filtragem

- Técnica apropriada para evitar a “tempestade de eventos (event storms)”;
- Consiste em suprimir um determinado alarme, em função dos valores de um conjunto de parâmetros, previamente especificados;
- Reduz o número de alarmes que são apresentados ao gerente de rede sem diminuir a habilidade do mesmo em reconhecer os problemas da rede.

Exemplo de filtragem



Falhas possíveis e filtragens de alarmes

- Servidor A
- Roteador 2
- Switch 3

Exemplo de filtragem

Status	Alarmes a filtrar
Servidor A fora	Servidor A fora até retorno do servidor A
Roteador 2 fora	Roteador 2 fora Switch 2 fora Roteador 1 fora Switch 1 fora Servidor A fora Servidor B fora
Switch 3 fora	Switch 2 fora Switch 3 fora Roteador 2 fora Roteador 1 fora Switch 1 fora Servidor A fora Servidor B fora

Contagem

- Contagem consiste em gerar um novo alarme a cada vez que o número de ocorrências de um determinado tipo de evento ultrapassar um limiar previamente estabelecido.

Escalação

- Escalação é uma operação na qual, em função do contexto operacional, um alarme é suprimido, sendo criado em seu lugar um outro alarme, no qual um parâmetro {p.ex., o parâmetro severidade) assume um valor mais alto.
- O contexto operacional inclui, dentre outros fatores, a presença de outros alarmes, o relacionamento temporal entre alarmes, o número de ocorrências de um evento em uma dada "janela" de tempo e as prioridades estabelecidas pelos gerentes da rede.

Generalização

- Generalização consiste em substituir um alarme, em função do contexto operacional, pelo alarme correspondente a sua super-classe
- Exemplo: na ocorrência simultânea de alarmes correspondentes a todas as rotas que utilizam como meio físico um determinado cabo, cada um dos alarmes originais pode ser substituído por um alarme indicando defeito no cabo; em seguida, através de uma operação de compressão, todos os alarmes repetidos podem ser substituídos por um alarme único.

Generalização

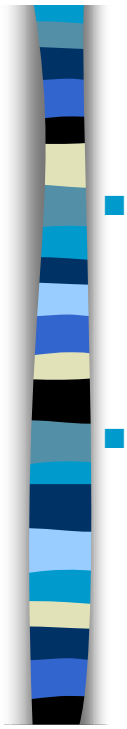
- Essa operação está baseada no raciocínio do tipo indutivo, o qual foi originalmente estudado por Aristóteles no século IV A.C.
- O raciocínio indutivo permite a ampliação do escopo do conhecimento, às custas do aumento da complexidade do problema e da introdução de um certo grau de incerteza no resultado da correlação.

Generalização

- Dois tipos principais de generalização podem ser identificados:
  - **generalização por simplificação de condições**
    - para que o alarme de classe mais baixa seja substituído por um outro de classe mais alta, são ignoradas ou desprezadas uma ou mais das condições definidas como necessárias à sua identificação. generalização baseada em instâncias
  - **generalização baseada em instâncias**
    - um novo alarme pode ser gerado a partir da associação das informações correspondentes a dois ou mais alarmes recebidos.

Especialização

- Especialização é uma operação inversa à generalização, que consiste em substituir um alarme por um outro, correspondente a uma sub-classe
- Esta operação, baseada em raciocínio do tipo dedutivo, não acrescenta novas informações em relação às que já estavam implicitamente presentes nos alarmes originais e na base de dados de configuração, mas é útil no evidenciamento das conseqüências que um evento numa determinada camada de gerência pode ocasionar nas camadas de gerência superiores.



Especialização

- Como exemplo de uma possível especialização, o sistema de correlação pode gerar, sempre que determinada rota for interrompida, um alarme para cada um dos serviços afetadas pela interrupção.
- Desta forma, através da especialização, estarão sendo evidenciadas conseqüências de uma falha na camada de gerência de rede de telecomunicações sobre entidades da camada de gerência de serviços de telecomunicações.

Relacionamento Temporal

- Relacionamento Temporal é uma operação na qual o critério para correlação depende da ordem ou do tempo em que são gerados ou recebidos os alarmes.
- Diversas relações temporais podem ser definidas, utilizando conceitos tais como:
  - DEPOIS-DE,
  - EM-SEGUIDA A,
  - ANTES-DE,
  - PRECEDE,
  - ENQUANTO,
  - COMEÇA,
  - TERMINA,
  - COINCIDE-COM,
  - SOBREPÕE-SE-A

Aglutinação

- Aglutinação consiste na geração de um novo alarme a partir da verificação do atendimento pelos alarmes recebidos, de padrões complexos de correlação.
- A operação de aglutinação também pode levar em consideração o resultado de outras correlações e o resultado de testes realizados na rede.

Objetivo da correlação

- Pode incluir desde a redução do volume de informações encaminhadas aos gerentes de redes até algo mais elaborado, tal como a localização e o diagnóstico de falhas, ou a predição do comportamento futuro da rede, baseada em análise de tendências.

Topologia do sistema de correlação

- Onde devem ser localizados os dispositivos correlatores e que tipo de relacionamento deve existir entre eles
  - **nível mais baixo: processos mais simples e mais rápidos.**
    - Por não levar em consideração o contexto mais amplo, esta classe de correlação sofre de uma acentuada "miopia" , que a impede de detectar possíveis reflexos que problemas locais podem ocasionar na rede como um todo.
  - **nível mais alto: todas as informações relevantes podem,ser oferecidas ao mecanismo correlator , que desta forma tem uma ampla visão do sistema gerenciado e pode diagnosticar problemas através dos seus reflexos sobre a rede como um todo.**
    - Em contrapartida, a grande quantidade de informações disponíveis provoca um aumento da complexidade do problema, que muitas vezes torna-se intratável.

Métodos e Algoritimos Para Correlação de Alarmes

- Correlação Baseada em Regras
- Lógica Difusa
- Redes Bayesianas
- Raciocínio Baseado em Modelos
- Quadro-negro
- Filtragem
- "Event Forwarding Discriminator" -EFD
- Raciocínio Baseado em Casos

Métodos e Algoritimos Para Correlação de Alarmes

- Correlação por Codificação
- Localização Explícita
- Correlação por Votação
- Correlação "Proativa”
- Correlação Distribuída
- Redes Neurais Artificiais
- Diagnóstico por Comparação de Resultados de Testes

Correlação Baseada em Regras

- 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 ligadas por um conectivo de implicação 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 regra altera o banco de dados.

Sistema especialista baseado em regras

- Um sistema especialista baseado em regras é mais simples, mais modularizado e mais fácil de manter, por ser organizado em três níveis:
  - 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.

Limitações dos sistemas baseados em regras

- 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")

Lógica Difusa

- 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.
- Exemplo
  - Se o tráfego na rota A estiver muito alto e o tráfego na rota B estiver norma desvie 1/4 do tráfego da rota A para a rota B;
  - A ocorrência do alarme C às vezes indica falha do equipamento D.

Lógica difusa

Exemplo de conversão de valores qualitativos em quantitativos

Tráfego (Erglang)	Grau de pertinência ao Conjunto
Até 30	0
30 a 40	0,2
40 a 50	0,4
50 a 60	0.6
60 a 70	0,8
70 a 80	0,9
80 a 90	0,95
90 a 100	1

Erlang: Medida de tráfego telefônico. Um erlang eqüivale a 1 hora completa, ou 3.600 segundos, de conversação telefônica.

Redes Bayesianas

- Uma rede bayesiana é um grafo acíclico dirigido no qual cada nodo representa uma variável aleatória à qual são associadas probabilidades condicionais, dadas todas as possíveis combinações de valores das variáveis representadas pelos nodos predecessores diretos;

Redes Bayesianas

- Uma aresta nesse grafo indica a existência de influência causal direta entre as variáveis correspondentes aos nodos interligados.

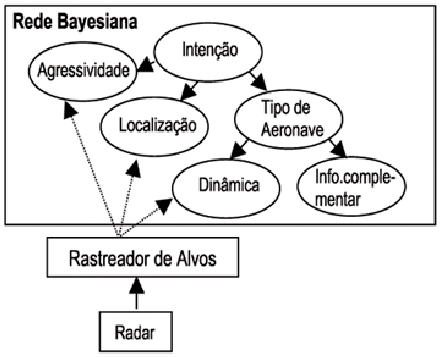


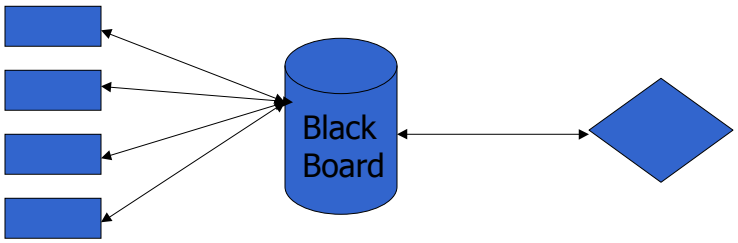
Figura 4: Modelo de uma rede bayesiana, destinada a obter o tipo do alvo rastreado e estimar suas intenções.

Raciocínio Baseado em Modelos

- Os princípios de MBR foram originalmente propostos em.
- MBR consiste em se representar um sistema através de um modelo estrutural e de um modelo funcional, em contraste com os sistemas baseados em regras tradicionais, onde as regras se baseiam em associações empíricas

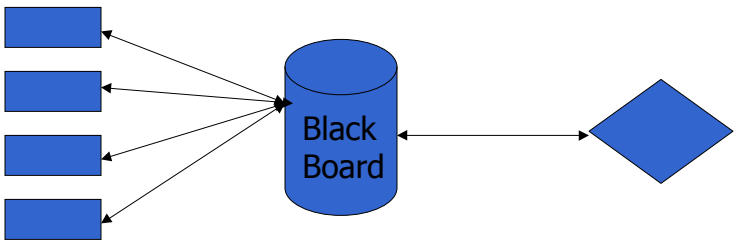
Quadro-negro (blackboard)

- O quadro-negro é responsável por armazenar elementos de solução ("solution elements") produzidos pelo sistema durante o processo de resolução do problema.



Brackboard

- Os elementos de solução são organizados no quadro-negro segundo dois eixos, representando níveis de abstração e intervalos de solução, respectivamente.



Filtragem

- Alguns sistemas de gerência de redes dispõem de filtros que selecionam as notificações alarmes a serem exibidas, a pedido do operador, segundo critérios tais como área geográficas 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, segundo o qual um filtro é um conjunto de asserções sobre a presença ou os valores atributos em um objeto gerenciado

Filtragem

- Existe uma modalidade de correlação de 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

"Event Forwarding Discriminator" -EFD

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

Raciocínio Baseado em Casos

- 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 e são armazenados, recuperados, adaptados e utilizados na solução de novos problemas.
- A experiência obtida com a solução destes novos problemas constitui novos casos, que são acrescentados ao banco de dados, para uso futuro.

Raciocínio Baseado em Casos

- Alternativa a abordagem baseada em regras, na qual tem-se:
  - Conjunto de Regras ⇔ Conhecimento
  - Conhecimento específico
  - Asserções armazenada em banco de dados
  - Um especialista define as regras
- Um *caso,* e não uma *regra,* é a unidade básica do conhecimento
- Casos ⇔ Registros de Episódios ⇔ Experiências ⇔ Conhecimento
- CBR - Case Based Reasoning

Características CBR

- Experiências obtidas com a solução de problemas constituem novos Casos
- Casos são inseridos em bancos de dados para acessos futuros
- O sistema adquire conhecimento por seus próprios meios
- Capaz de modificar comportamento futuro em função dos erros cometidos
- Construção de soluções para problemas inéditos através da adaptação de casos passados

CBR: Sinais de Invasão

- Processos estranhos na máquina
- Atividade acima do normal
- *Reboots* sem razão aparente
- Arquivos escondidos (“.“, “...”, etc)
- Entradas novas na base de dados dos usuários
- Novos servicos no inetd.conf
- Sua senha circulando no *underground*

Recuperando de uma Invasão

- Avalie a invasão
- Se existe suspeita do invasor ter-se tornado *root*, reinstale o sistema
- Recupere *backups* confiáveis
- Corrija a falha e reconecte a máquina na rede
- Avise os administradores dos sites envolvidos
- Avise grupo de segurança da área
- Faça relatório detalhado para a gerência (especificando o custo do ataque)
- Tome medidas legais, se for o caso

Proposta de Aplicação - I

Visão geral e Objetos MIB

- Detecção de invasões avaliando:
  - **Processos estranhos**
    - `HOST-RESOURCES-MIB`
      - `hrSystemProcesses`
      - `hrSystemMaxProcesses`
      - `hrSWRunName`
      - `SWRunType`
      - `hrSWRunStatus`

Proposta de Aplicação – II

Visão geral e Objetos MIB

- Detecção de invasões avaliando:
  - **Atividade acima do normal**
    - **HOST-RESOURCES-MIB**
      - **hrSWRunName**
      - **SWRunType**
      - **hrSWRunStatus**
      - **hrSWRunPerfCPU**
      - **hrSWRunPerfMem**
    - **RFC1213-MIB**
      - **If(In/Out)Octets**
      - **If(In/Out)UcastPkts**
      - **If(In/Out)NUcastPktsh**
      - **If(In/Out)Discards**
      - **If(In/Out)Errors**
      - **If(In/Out)UnknownProtos**

Proposta de Aplicação – III

Visão geral e Objetos MIB

- Detecção de invasões avaliando:
  - **Reboots sem razão aparente**
    - **RFC1213-MIB**
      - **sysUpTime**
      - **ifLastChange**
    - **HOST-RESOURCES-MIB**
      - **hrSystemUptime**
      - **hrSystemInitialLoadDevice**
      - **hrSystemInitialLoadParameters**

O que deve ser feito

- Definir situações “normais” de funcionamento do sistema e seus respectivos desvios padrões
- Iniciar base de dados com valores dos objetos em uma situação “normal”
- A cada alteração (observando desvios) inserir casos e determinar tipos de falhas
- Observar novas alterações e relacioná-las com casos já armazenados

Correlação por Codificação

- Na abordagem de codificação ("coding approach") [Kliger et al.) 1995] a maior 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 Pi = (S1,S2,...Sn) contém a medida de causalidade do problema Pi em relação ao sintoma correspondente.

Localização Explícita

- Cada alarme é explicitamente associada uma informação sobre localizações de falhas, consistindo de um conjunto que contém todas as localizações possíveis.
- Esta proposta guarda alguma semelhança com o modelo recomendado pelo ITU- T, o qual cada notificação de alarme pode conter, entre outras informações, um parâmetro denominado correlated notifications

Correlação por Votação

- Correlação por votação é uma técnica conceitualmente similar à técnica de localização explícita
- 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

Correlação "Proativa”

- Através das técnicas de garimpagem de dados ("data mining") e de descobrimento conhecimento ("knowledge discovery") é possível descobrir padrões que caracterizam o comportamento atual e as tendências de comportamento futuro da rede.
- A técnica de correlação proativa consiste em se varrer os dados disponíveis, sistemática e exaustivamente, aplicando técnicas de correlação e de aprendizado

Correlação 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 e trocam informações sobre o estado de seus domínios.

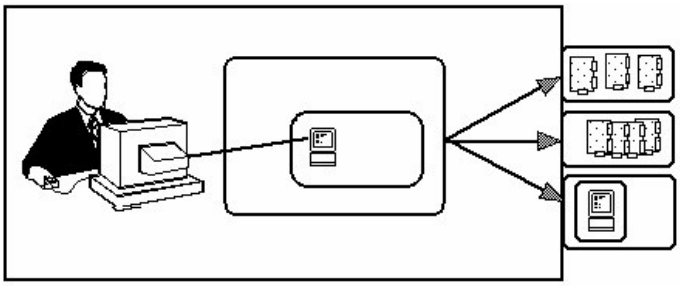
Redes Neurais Artificiais

- Uma rede neural artificial ("Artificial Neural Network" -ANN) é um sistema constituído de elementos ("neurônios") interconectados segundo um modelo que procura reproduzir a rede neural existente no cérebro humano.

Diagnóstico por Comparação de Resultados de Testes

- A técnica baseia-se em um "paradigma de teste por comparação" , que consiste em se fazer os nodos da rede executarem uma série de tarefas conhecidas.
- O diagnóstico dos nodos ou enlaces defeituosos é feito a partir das discrepâncias observadas nos resultados dos testes; a precisão do diagnóstico pode ser controlada através do número de vezes que a tarefa é repetida.

Exemplos de produtos



NerveCenter Pro

- Sistema NerveCenter Pro, da Seagate [Hewlett Packard, 1995a] [Seagate, 1996] utiliza "modelos de comportamento" para identificar problemas críticos, fazer correlação de alarmes e executar ações sobre a rede.
- As informações recebidas pelo sistema podem incluir mensagens SNMP ("traps" e "polls") quanto mensagens emitidas pelos sistemas HP Open View OperationsCenter ou Seagate LANAl

Sinergia

- Sinergia é um sistema especialista baseado em regras, utilizado no diagnóstico de falhas da rede de telecomunicações italiana.
- Através de correlação, em tempo real, de alarmes das redes de transmissão e de comutação, o sistema reduz em uma ordem de grandes quantidade de informações apresentadas aos operadores

TASA

- O sistema TASA (Telecommunication Alarm Sequence Analyzer) trabalha sobre o fluxo de alarmes gerado por um sistema de telecomunicações, buscando descobrir regularidades, ou seja, seqüências de alarmes que se repetem freqüentemente e, a partir daí, propondo regras que podem ser incorporadas a um sistema de correlação

TASA

- As regras propostas são do tipo: "se alarmes dos tipos alarme de enlace e falha de enlace ocorrem dentro de um intervalo de 5 segundos, então um alarme do tipo alta taxa , de falhas ocorre dentro de 60 segundos, com probabilidade 0.7".
- Através de uma interface hipertexto, o sistema TASA apresenta grande conjuntos de sugestões de regras (correspondendo às regularidades descobertas pelo sistema), dos quais diferentes visões podem ser oferecidas ao operador.
- As seleções das regras é feita interativamente, utilizando filtragem, ordenação e agrupamento.

InCharge (SMARTS)

- InCharge é um sistema completamente automático para diagnóstico de falhas em redes de telecomunicações ou de dados
- O sistema foi desenvolvido pela empresa norte-americana System Management ARTS Inc. - SMARTS e utiliza uma máquina de correlação baseada na abordagem de codificação, patenteada pela SMARTS

NetFACT (IBM)

- Através de correlação de alarmes, o sistema IBM NetFACT executa o diagnóstico e o acompanhamento da propagação de falhas em redes de telecomunicações.
- O sistema utiliza a técnica de correlação por votação, combinada com a pesquisa em árvores de dependências.
- O NetFACT opera no ambiente de gerência de rede NetView, da IBM

IMPACT (GTE)

- IMPACT (Intelligent Management Platforms for Alarm Correlation Tasks) é um sistema desenvolvido pela GTE utilizando a abordagem baseada em modelos
- A implementação tem como suporte um sistema especialista denominado ART- IM , conta com uma máquina de correlação baseada em regras e usa um algoritmo de encadeamento direto.

GMS

- Aplicação do raciocínio baseado em modelos na área de gerência de redes de telecomunicações, tomando como base o trabalho realizado nos projetos AIM (Advanced Information Processing (AIP) Application to IBCN (Integrated Broadband Communication Network) Maintenance) e GEMA (Generic Maintenance Ap- plication) do programa europeu RACE

GMS

- Sistema de gerência de falhas baseado em modelos denominado GMS (Generic Maintenance System), para a manutenção corretiva on-line de falhas de hardware.
- O GMS pode ser aplicado na manutenção de qualquer sistema de telecomunicações, desde que se use uma base de dados de conhecimento (modelo) específica para cada sistema.

ECXpert (AT&T)

- ECXpert: cuja função é ajudar os operadores de centros de gerência de rede na análise de alarmes e na tomada de decisões sob as ações corretivas a serem adotadas
- O ECXpert adota uma estrutura de dados denominada esqueleto de árvore de correlação (correlation tree sketelon) para representar um conjunto de alarmes que têm entre si uma relação de causa e efeito. Nestas árvores, uma ligação do tipo pai-filho equivale a um relacionamento causa-efeito entre alarmes

ECXpert

- Os esqueletos são usados como base para construir instâncias de árvores correlação (correlation tree instances) , a partir dos alarmes recebidos da planta, em tempo real.
- Portanto, o papel principal do ECXpert é receber alarmes e criar, dinamicamente árvores de correlação baseadas em esqueletos de árvore de correlação

SCOUT (AT&T)

- SCOUT é um sistema desenvolvido pelos Laboratórios Bell, da AT&T, para automatizar o diagnóstico de problemas de transmissão em redes de telecomunicações
- Um dos objetivos do produto é detectar e prever a ocorrência de problemas crônicos no sistema de transmissão, através do uso de técnicas de aprendizado, possibilitando a manutenção proativa desse sistema
- A arquitetura do SCOUT baseia-se no paradigma do quadro-negro

NOAA

- NOAA (Network Operations Analyzer and Assistant) é um sistema utilizado em gerência de tráfego na rede telefônica da Pacific Bell, no Estado da Califórnia
- NOAA é um sistema baseado em regras que também faz uso de técnicas de redes neurais

NOAA

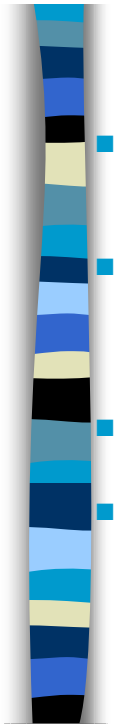
- A versão apresentada tem 120 regras e conta com um algoritmo, denominado ITRULE ("Information Theoretic Rule Induction") para aquisição automática de regras a partir dos bancos de dados de gerência de rede
- Também foram desenvolvidos recursos para lidar com as situações nas quais nenhuma regra se aplica. Nestes casos, o operador é convidado a entrar com novas regras ou a marcar aquela situação como um "caso especial" .

CRITTER

- Sistema de bilhetes de anormalidades que utiliza raciocínio baseado em casos para o diagnóstico de falhas na rede.
- Um banco de dados de bilhetes de anormalidades é uma bilioteca de casos.
- O componente CBR do sistema CRITTER provê mecanismos para se recuperar um bilhete útil, adaptá-lo (se isto for necessário para gerar uma recomendação de solução para o problema atual) e acrescentar o novo bilhete à biblioteca de casos.

FIXIT

- O sistema denominado FIXIT (Fault Information Extraction and Investigation Tool é uma arquitetura baseada em casos na qual a experiência adquirida em gerenciamento de falhas é codificada e colocada à disposição do pessoal



OPA - Operations Assistant

- Gensym Corporation desenvolveu o produto que funciona em conjunto com um outro software produzido pela empresa e denominado G2
- OPA é um sistema baseado em regras que pode analisar, filtrar, correlacionar e priorizar alarmes, o diagnóstico de falhas e a recomendação de ações corretivas aos operadores.
- Também é possível o reconhecimento de padrões, o que permite a manutenção proativa da rede
- OPA pode ser interfacetado com plataformas de gerência de rede tais como HP Open-View e IBM Net View. A AT&T desenvolveu um sistema integrado de gerência de rede utilizando Open View, junto com os softwares G2 e OPA.