Um Estudo sobre Correlação de Eventos em Redes de Telecomunicações

Linnyer Beatrys Ruiz[1] José Marcos Silva Nogueira[2]
Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
{linnyer, jmarcos}@dcc.ufmg.br

Resumo

A correlação de eventos é uma tecnologia amplamente aceita e foi principalmente usada para descoberta de falhas nas redes e análise de causa raiz. É importante ampliar a utilização da correlação de eventos para outras áreas funcionais de gerenciamento, quais sejam, desempenho, configuração, segurança e contabilização. Este estudo apresenta os principais conceitos, características, métodos e técnicas envolvidos com a correlação de eventos nas redes de telecomunicações. A correlação de eventos eficiente e precisa é essencial para reduzir o custo com a manutenção e melhorar a disponibilidade e o desempenho dos serviços das modernas redes de telecomunicações e redes de dados.

1 Introdução

Um ambiente de telecomunicações é composto de uma grande variedade de software e hardware em funcionamento, diversos protocolos, diferentes sistemas de supervisão, equipamentos de vários fabricantes e modelos distintos. A grande maioria dos componentes possui a capacidade de emitir mensagens referentes a eventos, isto é, avisos que relatam a criação ou destruição de objetos, trocas no valor do atributo, trocas no valor do estado e diferentes tipos alarmes (alarme de comunicação, alarme de qualidade de serviço, alarme de processamento, alarme de equipamento, alarme ambiental e alarmes proprietários) que podem apresentar diferentes níveis de severidade [ITU-T, 1996].

Em uma rede de telecomunicações, como em todo sistema complexo, existe uma intensa interdependência entre seus diversos componentes na execução dos serviços para os quais eles foram projetados. Pode-se dizer que existem diversos tipos de relacionamentos entre os elementos pertencentes a uma rede de telecomunicações. Por exemplo, um alarme emitido por um componente C1 pode estar relacionado com um problema ocorrido em C2 e, ao se solucionar o problema em C2, o alarme de C1 cessa. Em outra situação, a retirada de serviço de um equipamento gera alterações nas estruturas de dados que representam o equipamento, por exemplo a troca de valores de atributos ou a troca do seu estado administrativo, podendo provocar uma avalanche de eventos na rede que faz uso desse equipamento.

O rápido crescimento na quantidade de serviços fornecidos sobre a rede e o correspondente aumento dos recursos requeridos, representam um considerável desafio às novas aplicações de gerência para empresas modernas. O gerenciamento destas redes também aumentou em relação à sofisticação e magnitude. A motivação para incorporar alguma inteligência e automação de tarefas na infraestrutura de gerenciamento da rede é direcionada pela necessidade de continuar gerenciando e aumentando o tamanho da rede sem aumentar a equipe de operadores, pela necessidade de fornecer uma alta qualidade de serviço para os usuários garantindo que os objetivos do nível de serviço para rede serão mantidos, pela necessidade de correlacionar eventos das camadas inferiores de gerenciamento para determinar estratégias nas superiores, pela necessidade de aumentar a sofisticação requerida para diagnóstico, devido a maior complexidade do sistema e pela necessidade de detectar falhas na rede rapidamente e se possível a recuperação automática.

Como parte inicial da pesquisa, apresenta-se um estudo sobre a correlação de eventos, principais conceitos e características, tipos, aplicações e abordagens tecnológicas. A correlação de eventos é uma tecnologia amplamente aceita pois gerencia a complexidade das redes de telecomunicações e redes de dados. Este trabalho toma como ponto de partida a pesquisa realizada por

---

[1] Doutoranda em Ciência da Computação. Prof ª Adjunta da PUCPR.
[2] Orientador. Prof. Adjunto da UFMG

[Meira, 1997] envolvendo novas técnicas e abordagens e a proposição do uso da correlação de eventos para todas as áreas funcionais, isto é, deseja-se estender a correlação para todos os eventos da rede e com isto, não só retirar dos processos de gerência dados e informações, como também, conhecimento.

Para que uma rede de telecomunicações possa ser utilizada eficazmente, é indispensável que todos os seus recursos sejam adequadamente gerenciados e que haja integração entre as diversas áreas funcionais, quais sejam falhas, desempenho, configuração, segurança e contabilização e os diferentes níveis de gerência, sendo estes, gerência de elemento de rede, gerência de rede, gerência de serviços e gerência de negócios.

Este texto está organizado com a seguir. Na seção 2 faz uma breve descrição do cenário onde a correlação de eventos faz-se necessária. Na seção 3 estão expostas as motivações para a utilização da correlação na ocorrência de todos os eventos da rede. A seção 4 é dedicada aos conceitos, tipos de correlação, métodos e abordagens para correlação de alarmes. E a seção 5conclui o trabalho apresentado os desafios nesta área.

2 O Problema do Excesso de Eventos

Devido à interdependência entre componentes físicos e lógicos de um rede de telecomunicações, pode ocorrer uma situação crítica chamada de "tempestade de eventos" (*event storm*), onde acontece uma verdadeira avalanche de eventos e/ou alarmes. Tal cenário é essencial para integrar um sistema de correlação de eventos dentro da arquitetura de gerência da rede e com isto transformar eventos de rede em informação com valor adicional, habilitando operadores de rede a gerenciar a rede de forma eficiente. Um exemplo dessa "tempestade de eventos" está apresentado em [Fröhlich, 1997]: nas grandes redes de telefonia celular, como as atuais redes GSM (padrão das redes digitais de telefonia móvel que ligam os países europeus), em situações críticas, tais quais a passagem de uma tormenta, os vetores de alarmes tendem a inundar as estações de gerenciamento. As chuvas pesadas afetam a operação de enlaces de microondas, e a força eletromagnética dos relâmpagos ativa os comutadores de proteção usados para salvaguardar o equipamento eletrônico. O desempenho do serviço de telefonia móvel fica extremamente degradado em tais situações. Além disso, os operadores têm enorme dificuldade de interpretar quais são as notificações mais ou menos importantes. Em [Katker1997] encontra-se outro exemplo: "um cenário típico que compreende aplicações rodando sobre TCP/IP, usando tecnologia ATM, baseada em enlaces de transmissão SDH...". A quebra de um enlace no backbone ou qualquer outro problema no serviço básico de transmissão causará um grande número de falhas nos serviços de níveis mais altos. Esses serviços podem nem mesmo estar diretamente conectados ao componente que falhou, isto é, uma falha num enlace SDH pode provocar distúrbios na operação da rede TCP/IP e possivelmente grande número de conexões serão afetadas.

Todas as mensagens geradas na rede são enviadas a um centro de gerenciamento, onde os operadores analisam, entre outras coisas, os alarmes gerados e tentam solucioná-los. Um elemento físico ou lógico, envolvido no serviço de transporte de informações em uma rede de telecomunicações, pode gerar relatórios que descrevem a ocorrência do evento. Muitas vezes esta ocorrência provoca a emissão de um número muito grande de relatórios que é capaz de atingir a taxa de centenas por segundo, durante dezenas de segundos. Quando diversos elementos estão relacionados, esse número pode ser multiplicado e alcançar valores difíceis de serem suportados por sistemas de gerenciamento convencionais. A situação se agrava quando esses relatórios são enviados para um sistema remoto através dos meios de transmissão utilizados para o transporte de informações relativas aos serviços prestados. Esse tráfego volumoso de mensagens de gerenciamento pode ocasionar a queda de desempenho da rede, prejudicando o serviço para o qual a rede foi inicialmente projetada.

3 Motivação para Correlação de Eventos

Como visto, um problema grave e prático dos sistema e aplicações de gerência de redes é a gerência não apropriada de eventos. Os eventos enviados por um sistema gerenciado são frequentemente descritos como sintomas de um problema ao invés de sua causa. Mecanismos de filtragem de evento clássicos têm pouco impacto. O objetivo da correlação de eventos é reduzir o número de eventos

mostrados ao operador e enriquecer o significado dos eventos que são então mostrados. A correlação de eventos deve ser capaz de "sumarizar" os eventos que recebeu para um único evento que representa a ocorrência dos demais.

As técnicas convencionais envolvidas com o gerenciamento de eventos tratam do diagnóstico de falha, ou seja, envolvem apenas a área funcional de falhas e apoiam-se na experiência profissional dos operadores. É importante ampliar a utilização de correlação de evento para outros aspectos de gerência de rede e serviço, tal como desempenho, teste, qualidade de serviço, contabilização e gerenciamento de segurança. Por exemplo, na área de gerenciamento de segurança de rede de tempo real, a correlação de eventos pode ser usada para detecção de fraudes. Mais importante, a tecnologia de correlação deve estender-se entre diferentes domínios e níveis de gerência. Pode-se também citar como exemplo, a gerência de tráfego, onde uma aplicação demanda a coleta e o processamento de informações, em tempo real, com objetivo de detectar anomalias nos padrões de tráfego da rede e tomar as providências necessárias para remediá-las [Meira, 1997].

Pelo exposto, é evidente a necessidade de sistemas que possibilitem gerenciar eventos ou conjunto de eventos, correlacionando-os e fornecendo subsídios para a tomada de decisões, auxiliando na gerência da rede e envolvendo todos os níveis de gerência e todas as áreas funcionais e não apenas a gerência de falhas.

4 Correlação de Eventos

Correlação de eventos eficiente e precisa é essencial para reduzir custo com manutenção da rede e melhorar a disponibilidade e o desempenho dos serviços da rede. Dados brutos são interpretados e analisados, levando em consideração um conjunto de critérios pré-estabelecidos, ou definidos dinamicamente em função do processo de gerência.

Alguns autores [Kehl e Hopfmüller,1993 *apud* Meira,1997] definem correlação como um processo no qual se cria um conjunto mínimo de hipóteses de falhas para um dado conjunto de alarmes. Porém um alarme nem sempre está associado a uma falha. Em [Jakobson e Weissman, 1993 *apud* Meira, 1997] a correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais. A correlação tem como objetivo reduzir a quantidade de notificações de eventos transferidas aos operadores do sistema de gerência de rede, aumentando o conteúdo semântico das notificações resultantes e realizando a previsão quanto à ocorrência de falhas no futuro.

4.1 Tipos De Correlação

Diversos tipos de correlação podem ser identificadas em função das operações executadas sobre os alarmes disponíveis. As mais importantes destas operações são detalhadas[Jakobson e Weissman, 1995]:

Compressão

Compressão consiste em detectar, a partir da observação dos eventos recebidos em uma dada janela de tempo, múltiplas ocorrências de um mesmo evento, substituindo os eventos correspondentes por um único evento, 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 - relacionado ao contexto dinâmico do processo de gerência de rede. Os critérios de supressão geralmente estão vinculados à presença de outros eventos, ao relacionamento temporal entre alarmes ou a prioridades estabelecidas pelos gerentes da rede.

Filtragem

Filtragem consiste em suprimir um determinado evento, em função dos valores de um conjunto de parâmetros, previamente especificados. Em um sentido restrito, a filtragem leva em consideração apenas os parâmetros do evento que estiver sendo filtrado sendo que este tipo de correlação pode

considerar quaisquer outros critérios. Neste caso, o conceito de filtragem se expande podendo englobar outros tipos de operações, tais como compressão e supressão.

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 a operação na qual, em função do contexto operacional, um evento é suprimido, sendo criado em seu lugar um outro evento, no qual um parâmetro assume valores mais altos. O contexto operacional inclui, entre outros fatores, a presença de outros eventos, o relacionamento temporal entre eventos, 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 evento, em função do contexto operacional, pelo evento correspondente a sua *super-classe* [Bapat, 1994 *apud* Meira, 1997].

Dois tipos principais de generalização podem ser identificados: generalização por simplificação de condições e generalização baseada em instâncias [Holland *et al*., 1986 *apud* Meira, 1997]. No primeiro caso, para que o evento da classe mais baixa seja substituído por um outro de classe mais alta no diagrama de classes, são ignoradas ou desprezadas uma ou mais condições definidas como necessárias à sua identificação. No segundo caso, um novo evento pode ser gerado a partir da associação das informações correspondentes a dois ou mais eventos recebidos.

Especialização

Especialização é uma operação inversa à generalização, que consiste em substituir um evento por outro, correspondente a uma sub-classe [Bapat, 1994 *apud* Meira, 1997]. Esta operação, baseada em raciocínio do tipo dedutivo, não acrescenta novas informações em relação às que já estavam implicitamente presentes nos eventos originais e na base de dados de configuração, mas é útil no evidenciamento das consequências que um evento numa determinada camada de gerência pode ocasionar nas camadas de gerência superiores.

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 eventos. Diversas relações temporais podem ser definidas, utilizando conceitos 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 evento a partir da verificação do atendimento, pelos eventos 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.

4.2 Métodos e Algoritmos para Correlação de Eventos

O trabalho envolve a pesquisa das principais abordagens existentes na literatura, classificadas segundo os métodos e algoritmos utilizados no processo de correlação [Meira, 1997]. Desta forma, o trabalho de pesquisa envolveu o estudo a respeito das diferentes abordagens disponíveis. Entre outras, fizeram parte da pesquisa as seguintes abordagens: Correlação Baseada em Regras, Correlação utilizando Lógica Difusa ("*fuzzy logic*"), Redes Bayesianas ou Redes Causais, Raciocínio Baseado em Modelos, Quadro-negro ("*blackboard*"), Filtragem, "*Event Forwarding Discriminator*" - EFD, Raciocínio Baseado em Casos, Correlação por Codificação, Correlação por Localização Explícita, Correlação por votação, Correlação "Proativa", Correlação Distribuída, Correlação Distribuída Baseada em Serviço, Correlação Distribuída Baseada em Políticas, Redes Neurais Artificiais, Diagnóstico por Comparação de Resultados, Análise de Causa Raiz, Correlação utilizando Mineração de Eventos, Correlação baseada no Modelo Transversal, *Cross-Correlation*, Correlação Canônica, Raciocínio Hierarquico, Correlação utilizando *Rough Set*, Correlação baseada na Representação Formal de Dependências, Redes de Petri.

5 Conclusão

O desafio deste trabalho é investigar as possibilidades de disponibilizar a correlação de eventos, não somente para o gerenciamento de falhas através da correlação de alarmes, mas também envolver os eventos das demais áreas funcionais e níveis de gerência. Os obstáculos e as dificuldades estão associadas ao entendimento das próprias redes, pois existe uma carência de ferramentas que facilitem a modelagem de uma rede de telecomunicações, nos aspectos referentes à propagação dos efeitos dos eventos em suas sub-redes. A travessia de uma rede por todas as fontes de eventos reportados, causa duplicação de trabalho e uma alta demanda de por parte dos operadores que por vezes, estão diante de uma tempestade de eventos.

O cenário atual não possui habilidade para integrar ações que colecionem e avaliem informação de eventos. Os sistemas e seus componentes possuem, quando muito, um processo de correlação de alarmes. Aplicações específicas de correlação tem sido desenvolvidas para gerenciar redes comutadas de serviços, switches, ATM, SONET, IP, entre outras. Todos os maiores desenvolvedores na área de gerenciamento de redes tem desenvolvidos seus próprios, usualmente embutidos, procedimentos de correlação ou tem usado produtos tais como NeverCenter (http://www.veritas.com), InCharge (http://www.smarts.com), NetFACT (http://www.ibm.com), IMPACT (http://www.gte.com), ECXPert (AT&T), SCOUT (AT&T), ECS (http://www.openview.com), ART-Enterprise (ART*Enterprise).

5.Referências:

[Bapat, 1994] Bapat, Subodh. *Object-Oriented Networks*: Models for Architecture, Operations, and Management. NJ, USA: PTR Prentice Hall, Englewood Cliffs, 1994.

[Fröhlich,1997] Fröhlich, Peter et al.. *Model-based alarm correlation in cellular phone networks*. 1997. http:// www.kbs.uni-hannover.de/paper/96/mascot97/mascot97.html.(06 Jun. 1997, 17:54).

[Holland et al. 1986] Holland, John H. *et al*. Induction: Process of Inference, Learning and Discovery. The Massachusetts Institute of Technology, Cambridge, USA, 1986.

[ITU-T1996] ITU-T. Recommendation M.3010: Principles for a Telecommunications Management Network, May, 1996.

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

[Jakobson e Weissman, 1995] Jakobson, Gabriel e Weissman, Mark. Real time telecommunication network manegement: extending event correlation with temporal constraints. *In IFIP/IEEE International Symposium on Integrated Network Management*, IV, 1995, p. 290-301.

[Kätker,1997] Kätker, S. e Paterok, M.. Fault isolation and event correlation for integrated fault management. *In: Integrated Network Management V -Integrated management in a virtual world. IM'97 - sponsored by IFIP TC6 WG6 on Network Management e co-sponsored by the IEEE Communications Society*. San Diego, California, U.S.A., p. 584-587, may, 12-16 1997.

[Kehl e Hopfmüller, 1993] Kehl, Walter e Hopfmüller, Heinrich. Model-based reasoning for the manegement of telecommunication networks. *In IEEE International Conference on Communications*'93, p. 13-17.

[Meira, 1997] Meira, Dilmar Malheiros. *Um Modelo para correlação de alarmes em redes de telecomunicações*. 1997. 151f. Tese (Doutorado em Ciência da Computação) – Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Belo Horizonte.