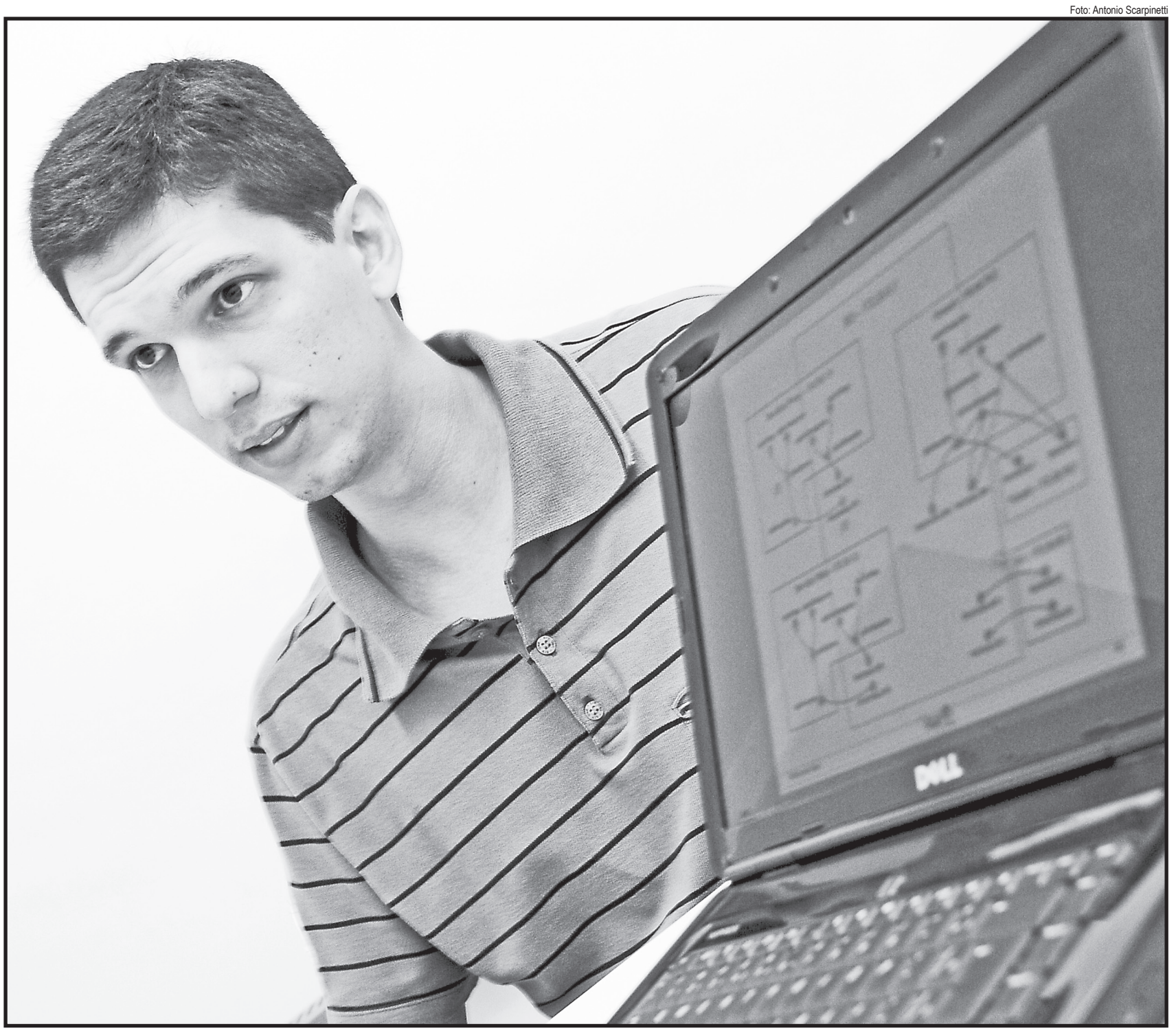
Sistema computacional dispara alarme sobre anomalias na rede

Software desenvolvido na Feec oferece ao administrador um cenário completo do problema

JEVERSON BARBIERI
jeverson@unicamp.br

Foto: Antonio Scarpinetti



Com mais de 60 milhões de usuários, a internet brasileira é considerada atualmente a quinta maior do mundo em número de conexões. Isso pressupõe um tráfego intenso de dados que, em determinados momentos, são responsáveis por causar desvios súbitos e acentuados no comportamento das redes, conhecidos como anomalias. Exemplos comuns disso são os bugs em softwares, o uso abusivo dos recursos computacionais, as falhas nos equipamentos, as configurações erradas e, ainda, os ataques feitos por hackers. Esses acontecimentos fizeram surgir a expressão "caiu a rede".

A visualização de todo esse conjunto permitiu ao analista de sistemas Bruno Bogaz Zarpelão o desenvolvimento de um sistema computacional de detecção de anomalias. Além de identificar de maneira mais simplificada a ocorrência, o software oferece ao administrador de rede um cenário completo do problema, facilitando a busca pela origem da anomalia e sua consequente solução no menor espaço de tempo possível. A pesquisa culminou com a tese de doutorado do pesquisador, orientada pelo professor Leonardo de Souza Mendes, da Faculdade de Engenharia Elétrica e de Computação (Feec).

Zarpelão explicou que nas redes de computadores atuais, que assumiram uma posição de grande importância no cotidiano de ambientes acadêmicos, governamentais e corporativos, detectar e tratar essas ocorrências de maneira eficiente se tornou uma tarefa fundamental. Uma das chaves do trabalho foi considerar o que é ou não uma anomalia. Esse limite, de acordo com o analista, foi deixado em aberto sob a justificativa de que cada administrador sabe o que quer para sua rede.

Dessa maneira, através da observação do número de bytes e pacotes que trafegam diariamente, é possível fazer uma análise estatística determinando o padrão de comportamento daquela rede. A partir daí, a percepção de um comportamento anormal pode gerar um alarme para o responsável tomar as devidas providências. Em grandes ambientes, explicou Zarpelão, é humanamente impossível tomar conta de todo o parque computacional, uma vez que o número de máquinas é bastante elevado. Após o acionamento do alarme, as ações previstas no plano de contingência são tomadas, como a ativação de um servidor de backup ou mesmo a troca de um equipamento queimado.

Em cada equipamento são monitorados diferentes indicadores, conhecidos como objetos de gerência. Um problema na rede afeta, em geral, o comportamento de vários objetos de gerência em vários equipamentos. Entregar ao administrador de redes os alarmes gerados para cada um destes objetos acabaria por sobrecarregá-lo. No trabalho de Zarpelão, foram levantados os relacionamentos entre estes indicadores, de forma que os alarmes gerados para cada um deles possam ser analisados em conjunto, levando à geração de um único alarme que traz informações sobre o comportamento de toda a rede. "Uma situação na qual o sistema gerou, inicialmente, 170 alarmes ao monitorar os objetos de gerência pode, a partir da análise destes alarmes iniciais, ter uma redução para apenas 15, os quais trazem o panorama de toda a rede, sem que se perca qualquer informação", assegurou.

Ainda com relação ao alarme, o pesquisador explicou que ele pode ser configurado para tocar em determinados dias quando a quantidade de tráfego da rede está pouco acima do padrão ou mesmo somente quando a situação já se encontre em um nível de gravidade bastante adiantado. "O software dá a liberdade ao administrador de escolher quando quer ser alertado sobre as mudanças de comportamento de sua rede", afirmou Zarpelão. Isso significa que o produto da pesquisa é permissível a alterações de sensibilidade, que na literatura é chamada de "níveis de sensibilidade de detecção". Assim, o administrador pode configurá-lo para que ele se adapte à sua política de gerenciamento.

Ele citou um caso exemplar, ocorrido em 11 de setembro de 2001, durante o ataque terrorista às torres gêmeas, em Nova York (EUA). O portal de notícias da rede CNN foi repentinamente acessado por muitas pessoas em busca de informações. O resultado foi que o portal caiu e ninguém mais conseguia acessá-lo por causa de uma sobrecarga. Nesse caso, o software desenvolvido por Zarpelão poderia emitir um alarme quando o número de acessos estivesse acima do padrão. O administrador teria condições de distribuir a carga para outras máquinas ociosas, ajudando a liberar o tráfego. "É uma coisa de momento, que pode gerar uma decisão capaz de ajeitar o cenário", disse.

Protocolo

Pela natureza das redes municipais existentes – locais onde o software deve ter sua utilização mais acentuada – o analista de sistemas contou que o desenvolvimento do produto se deu muito em função do padrão de gerência de redes, que é um protocolo chamado SNMP (Simple Network Management Protocol). Não há, segundo Zarpelão, uma solução no âmbito da literatura que trate o problema do começo ao fim, como o que foi feito por ele utilizando apenas o SNMP. "Tentamos explorar ao máximo esse padrão", ressaltou.

Esse direcionamento deu uma tranquilidade ao pesquisador, uma vez que o SNMP está disponível na maioria dos equipamentos comercializados, portanto, isso reduz um possível problema de implantação do software nas redes. Ele disse também que existem outros trabalhos publicados que usam como base para coleta de informações da rede métodos mais sofisticados como o NetFlow. "São métodos realmente melhores, no entanto, não são padrão e, dessa forma, não estão em todos os equipamentos. Isso dificulta a adoção de outras propostas", ressaltou Zarpelão.

Os testes do sistema computacional foram feitos com dados reais da rede da Universidade Estadual de Londrina (UEL), onde o coorientador de Zarpelão é docente. Como eles já possuem um projeto de pesquisa relacionado a esse tema, o pesquisador pode utilizar os dados daquela rede. "Está composta por cerca de seis mil estações de trabalho, unindo todos os departamentos, com bastante tráfego agregado, tornando-se assim, um ambiente bom de trabalhar", resumiu.

Ele contou que, também na UEL, já houve sobrecarga do servidor por conta da divulgação do resultado do vestibular. Todo mundo quer acessar ao mesmo tempo e, segundo o analista, ficou perceptível que a utilização do software poderia ter contribuído para que esse problema não ocorresse. O sistema identificou ainda situações como download de arquivos feitos por determinadas máquinas, o que pode ou não ser permitido pela gerência de rede.

Zarpelão tem como objetivo agora evoluir esse estudo um pouco mais, não só na questão da interface gráfica como na aplicação prática do software. Ele informou que outros alunos do Laboratório de Redes de Comunicações (LaRCom) da Feec já estão trabalhando no sentido de fornecer uma ferramenta ao administrador que contenha gráficos, que mostre o diagrama da rede e os respectivos alarmes.

O analista de sistemas Bruno Bogaz Zarpelão: análise estatística determina o padrão de comportamento da rede

Com relação a parte prática, Zarpelão informou que assim que a tecnologia desenvolvida por ele estiver mais madura deverá ser implantada no projeto Infovias Municipais, desenvolvido pelo LaRCom – Unicamp sob a coordenação do professor Leonardo de Souza Mendes. Neste projeto, todos os prédios públicos são interconectados por uma rede de fibra óptica e rádio-frequência. Para o analista, esse será um excelente teste. "Quando o projeto da Infovia saiu, minha pesquisa de doutorado já estava em estado bastante adiantado. Como tínhamos todos os dados da UEL resolvemos não abrir mão. Vimos que o software se comportou muito bem", concluiu.

Artigos

- Zarpelão, Bruno Bogaz ; MENDES, Leonardo de Souza ; Proença Jr., Mario Lemes . Anomaly Detection Aiming Pro-Active Management of Computer Network Based on Digital Signature of Network Segment. *Journal of Network and Systems Management*, v. 15, p. 267-283, 2007
- ZARPELÃO, Bruno Bogaz ; MENDES, Leonardo de Souza ; PROENCA JR., Mario Lemes ; RODRIGUES, Joel J. P. Coelho . Three Levels Network Analysis for Anomaly Detection. In: 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2009), 2009, Split-Hvar-Korcula, Croatia. Proceedings of 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2009), 2009.
- ZARPELÃO, Bruno Bogaz ; MENDES, Leonardo de Souza ; ABRAÃO, Taufik ; SAMPAIO, Lucas D. H. ; LIMA, Moisés Fernando ; PROENCA JR., Mario Lemes . Detecção de Anomalias em Redes de Computadores. In: XXVII Simpósio Brasileiro de Telecomunicações - SBrT 2009, 2009, Blumenau, SC. Anais do XXVII Simpósio Brasileiro de Telecomunicações, 2009.
- ZARPELÃO, Bruno Bogaz ; MENDES, Leonardo de Souza ; PROENCA JR., Mario Lemes ; RODRIGUES, Joel J. P. Coelho . Parameterized Anomaly Detection System with Automatic Configuration. In: IEEE Global Telecommunications Conference (GLOBECOM), 2009, Honolulu. Proceedings of IEEE Global Telecommunications Conference 2009, 2009.

Publicação

Tese "Detecção de anomalias em redes de computadores"
Autor: Bruno Bogaz Zarpelão
Orientador: Leonardo de Souza Mendes
Unidade: Faculdade de Engenharia Elétrica e de Computação (Feec)
Fonte de financiamento: Fapesp