Um Agente de Software Orientado à Monitoração de Traços de Protocolos. Ricardo Nabinger Sanchez, Luciano Paschoal Gaspary. (Programa Interdisciplinar de Pós-Graduação em Computação Aplicada. UNISINOS)

Nos últimos anos a proliferação de protocolos e aplicações para redes de computadores fez com que um número expressivo de usuários as incorporasse em seu uso cotidiano. Nesse contexto, ferramentas para caracterização e medição de tráfego tornaram-se essenciais sobretudo para justificar custos com a ampliação e manutenção da infraestrutura de rede. Muitos dos problemas enfrentados atualmente em redes como falhas, baixo desempenho e insegurança, são originados no uso incorreto dos protocolos e nas implementações deficientes dos aplicativos, de modo que caracterizar e medir o tráfego de rede não é mais suficiente para garantir o bom funcionamento dos protocolos e aplicações. Para amenizar esta problemática, está em desenvolvimento um agente de monitoração capaz de contabilizar seqüências de trocas de pacotes (traços), utilizando uma abordagem *stateful inspection.* Esta abordagem permite identificar comportamentos de interesse para a gerência de falhas, desempenho e segurança de forma precisa. Isto é possível porque, ao invés de avaliar cada pacote isoladamente, o agente passa a correlacionar pacotes pertencentes ao mesmo evento. As seqüências a serem analisadas (traços de protocolos) são especificadas pelo administrador de rede usando a linguagem PTSL (*Protocol Trace Specification Language*). Como exemplo, o agente pode ser usado no contexto de segurança atuando como um sistema de detecção de intrusão (IDS), desde que seja alimentado com especificações de traços de protocolos que representem cenários de ataques (Pibic/CNPq).