III SALÃO DE ENSINO E DE EXTENSÃO
2012 Vivenciando a Integração
ISSN 2237-9193
22 a 26 de Outubro de 2012

MONITORAMENTO ADAPTATIVO DE REDES DE COMPUTADORES BASEADO EM BPM

CARINE GEHLEN
carine@viavale.com.br
JOSE JAIR CARDOSO DE SANTANNA
josejair@unisc.br

A evolução das redes de computadores vem sendo acompanhada e motivada pelas demandas que as aplicações têm exigido. Para garantir o desempenho das redes é fundamental que o seu gerenciamento seja realizado constantemente. Esse gerenciamento está associado à atividade de controle dos recursos das redes (*e.g.,* banda disponível). Para efetuar o controle dos recursos outra atividade fundamental é o monitoramento. Existem duas formas de realizar o monitoramento de redes: forma intrusiva e não intrusiva. A primeira, intrusiva, é baseada em protocolos padronizados (*e.g.,* Simple Network Management Protocol - SNMP e Remote Monitoring - RMON) que possibilitam o acesso aos dispositivos através da comunicação gerente/agente. Entretanto, o monitoramento intrusivo adiciona tráfego de dados à rede e consome recursos que deveriam ser disponibilizados unicamente para os usuários. A segunda forma de gerenciamento, não intrusiva, não adiciona nenhum tráfego à rede e realiza o monitoramento baseado em observações de dispositivos que concentram o tráfego. Aplicações que disponibilizam essa observação são chamadas de *sniffers* de rede. *Sniffers* de redes atuais disponibilizam o monitoramento de duas formas distintas: (i) baseado em pacotes e (ii) baseado em fluxos. A principal diferença entre essas duas formas é que na primeira todas as informações dos pacotes são preservadas, permitindo uma maior precisão para a análise; já na segunda, os pacotes que possuem mesmas características (*i.e.,* porta, endereço de origem e de destino), são agrupados em um único fluxo. A escolha de qual a melhor dentre essas duas formas depende, unicamente, de qual granularidade deseja-se observar. Tráfegos que não apresentam nenhuma característica maliciosa ou desconhecida (considerando um histórico predeterminado) são mais indicados de serem monitorados por fluxo, pois consomem menos recursos para armazenamento e menor processamento das informações, nos outros casos o monitoramento em nível de pacote é mais indicado. Portanto, o objetivo principal deste trabalho é investigar uma abordagem adaptativa para o monitoramento não intrusivo. Para realizar a adaptabilidade do monitoramento não intrusivo é utilizada a abordagem chamada de gerenciamento de processos de negócios (i.e*., Business Process Management* - BPM). Essa abordagem disponibiliza a composição de um conjunto de tarefas, sendo que cada uma dessas tarefas, em geral, é uma operação de uma arquitetura orientada a serviço *(Service Oriented Architecture* - SOA). Então, com o objetivo de utilizar *sniffers* baseados em SOA como tarefas, primeiramente é realizado um estudo comparativo entre os principais *sniffers*, orientados a pacote ou a fluxo. Uma vez escolhidos os principais *sniffers*, é implementado o mecanismo adaptativo. Espera-se, como resultado, demonstrar quantitativamente que, através do mecanismo proposto, o monitoramento de redes é realizado de forma mais otimizada, isto é, utiliza menos espaço de armazenamento e menor poder de processamento sobre os dados monitorados.

Instituição: UNISC - SANTA CRUZ DO SUL/RS