FLOW-CHECKER: UM *FRAMEWORK* PARA ANÁLISE DE FLUXOS UTILIZANDO ARQUIVOS PCAP

Monteiro, Anderson[1](PG), Garcia, Vinícius F.[1](PG) , Tavares, Thales N.[1](PG), Silva, Nilton C. B.[1](PG), Marcuzzo, Leonardo da C.[1](PG), Lucca, Luísa Perin (G), Santana, Brenda Salenave (G), Santos, Carlos R. P.[1](O)

[1]*Departamento de Computação Aplicada – Grupo de Redes e Computação Aplicada, Universidade Federal de Santa Maria;*

O tratamento igualitário entre os diferentes fluxos de rede que passam por ISPs, sem benefício ou prejuízo caracterizado pela origem, destino, porta ou tipo de serviço dos pacotes, é o que conceitua neutralidade de rede. Nesse contexto é fundamental compreender as técnicas e motivações dos vários tipos possíveis de discriminação de fluxos e como estas técnicas são aplicadas na prática. Para que tais pontos sejam exclarecidos é necessário que análises sejam executadas encima de tráfegos simulados e tráfegos reais afim de determinar características comuns que possam caracterizar a quebra de neutralidade da rede. A solução Flow-Checker consiste de um *framework* para análise de fluxos TCP a partir de pacotes coletados através de *sniffers* de rede e convertidos para formato CSV. O framework tem o objetivo de realizar uma análise multi-variável aplicada a cada fluxo detectado. Como saída, o algoritmo converte os dados obtidos realizando uma apresentação através de gráficos facilitando a análise e compreensão humana. O framework apresenta três módulos principais: o de separação de fluxos, de análise e obtenção de métricas e a geração dos gráficos. O módulo de separação de fluxos consiste na discriminação dos mesmos a partir de um documento de pacotes unificados, um fluxo é caracterizado pela quintupla (IPOrigem, IPDestino, PortaOrigem, PortaDestino, Serviço) e para cada fluxo um novo documento CSV é gerado contendo todos os pacotes referentes ao mesmo. O módulo de obtenção de métricas analisa a saída gerada pelo módulo de de separação de fluxos, para cada fluxo detectado são computadas informações de *throughput*, latência, *jitter* e perda. Diversas soluções utilizam apenas uma métrica para analisar se há ou não quebra de neutralidade, porém, uma análise multi-variável oferece maior precisão tanto na detecção quanto na investigação de possíveis causas e efeitos desse fenômeno. Finalmente, o módulo de geração de gráficos utiliza os dados apresentados como saída do módulo de obtenção de métricas para ajustar parâmetros de gráficos LaTeX utilizando a biblioteca TikZ, esses gráficos são compilados. Após se ter os gráficos gerados pela ferramenta é possível realizar a comparação entre os fluxos de rede, sendo assim, facilitando o diagnóstico da realização de discriminação de algum tipo de conteúdo por parte do provedor de serviço e de tal forma estar havendo uma quebra de neutralidade.