11º FEPEG FÓRUM ENSINO · PESQUISA EXTENSÃO · GESTÃO
UNIVERSIDADE, SOCIEDADE E POLÍTICAS PÚBLICAS
ISSN: 1806-549X

ANÁLISE DE TRÁFEGO DE INTERNET A PARTIR DA INTERCEPTAÇÃO E MEDIÇÃO DE PACOTES COM UM SISTEMA DESENVOLVIDO EM JAVA

Autores: VITOR GIOVANE PEREIRA ALVES, NILTON ALVES MAIA

Introdução

A quantidade de usuários de *internet* no mundo está crescendo em ritmo acelerado. Face a esse crescimento a área de Análise de Tráfego de *Internet*, tema deste trabalho, apresenta grande demanda por novas tecnologias que apresentem melhores condições para suportar o tráfego intenso, proporcionar mais segurança aos usuários e maior disponibilidade dos serviços que utilizam a rede.

Para que se realize planejamentos eficientes que objetivem criar melhorias para uma rede de computadores é preciso munir-se de técnicas e ferramentas que possam de alguma forma fornecer informações que apresentem as características da rede. Diante do exposto, este trabalho teve o objetivo de analisar o tráfego de *internet* gerado nos laboratórios de informática do Centro de Ciências Exatas e Tecnológicas (CCET) da UNIMONTES, a partir da interceptação de pacotes TCP/IP, que segundo [1] é a pilha de protocolos da *internet*, e medição desses pacotes.

Material e métodos

A. Sistema TEOS

Desenvolveu-se um sistema na linguagem de programação Java intitulado TEOS, que possui três componentes: o Interceptador, o Calculador de vazão e o Calculador de perda de pacotes.

O Interceptador é responsável por capturar os pacotes TCP/IP de uma interface de rede selecionada pelo usuário, criar uma conexão com uma base de dados informada pelo usuário, criar nessa base uma tabela de nome escolhido pelo usuário e armazenar nessa tabela dados pertinentes a cada pacote interceptado, como IP de origem, IP de destino e tamanho do pacote em bytes. Por apresentar a característica de captura de tráfego de rede, o Interceptador é considerado uma espécie de *sniffer*, que, de acordo com [2], é um tipo de programa especial capaz de permitir a visualização de todo o tráfego de uma rede.

O Calculador de vazão é responsável por realizar um cálculo de vazão por hora, dado em *bits* por segundo (*bps*), para um determinado IP de origem e IP de destino. Já o Calculador de perda de pacotes é responsável por realizar um cálculo percentual de pacotes perdidos por hora, entre um IP de origem e um IP de destino. A interface do sistema TEOS é apresentada na Figura 1.

B. Ambiente de interceptação

O ambiente utilizado para a execução do Interceptador consistiu no servidor *gateway* do CCET que tem acesso bidirecional ao tráfego dos cinco laboratórios aos quais os acadêmicos e professores têm acesso à *internet*. Antes de iniciar-se a execução do Interceptador, fez-se necessário realizar instalações e configurações que garantissem a existência de um ambiente propício para a interceptação.

C. Medição de tráfego

ISSN: 1806-549X

No período entre 10h:36m:48s do dia 10 de julho de 2017 e 11h:26m:25s do dia 20 de julho de 2017, totalizando 10 dias, 0 horas, 49 minutos e 37 segundos, os pacotes TCP/IP dos computadores contidos nos laboratórios 1, 2, 3, 4 e 5 do CCET foram interceptados, utilizando-se o componente Interceptador do sistema TEOS, e armazenados na tabela "CCET" da base de dados TEOS. A autorização para o acesso à rede de dados do CCET, para efeitos de realização deste trabalho, foi concedida pela Direção do CCET.

Com o objetivo de medir e analisar o tráfego referente ao período de uma semana, considerou-se somente os pacotes interceptados entre 00h:00m:00s do dia 13 de julho de 2017 e 23h:59m:59s do dia 19 de julho de 2017, totalizando 7 dias, 0 horas, 0 minutos e 0 segundos de tráfego interceptado. Após o processamento dos dados e a obtenção dos resultados de vazão e perda de pacotes, gerou-se gráficos que exibem resultados hora a hora para cada dia analisado.

Resultados e discussão

A. Medição do tráfego

Utilizando-se o Interceptador, foram interceptados treze milhões, seiscentos e dezenove mil, setecentos e quarenta e dois pacotes TCP/IP, e, para cada um destes, gerou-se um registro na base de dados TEOS que apresentou o tamanho de 1,5 GB em arquivo SQL.

No dia 19, quarta-feira, obteve-se o maior fluxo de pacotes TCP/IP durante o período considerado, ao todo 1.780.701 pacotes. No dia 13, quinta-feira, foram interceptados 1.403.549 pacotes TCP/IP. Os dias 15 e 16 representam semanalmente o sábado e o domingo, respectivamente. Embora nesses dias espera-se um menor fluxo de alunos na UNIMONTES e consequentemente um menor fluxo de tráfego de *internet*, foram interceptados no sábado 1.225.442 pacotes TCP/IP e no domingo 1.246.120, valores individualmente superiores aos obtidos na terça e sexta-feira. No dia 14, sexta-feira, obteve-se a menor quantidade de pacotes TCP/IP, 1.031.617, já no dia 17, segunda-feira, obteve-se 1.763.356. Obtiveram-se 1.061.475 pacotes TCP/IP no dia 18, terça-feira, número equivalente à segunda menor quantidade de pacotes interceptados.

B. Resultados de vazão e perda de pacotes

Os resultados de vazão e perda de pacotes foram expressos, para cada dia interceptado, em gráficos. Como pode ser observado nos Gráficos 1 e 2, o identificador de intervalo "0" equivale ao intervalo 00h00m00s à 00h59m59s, o identificador de intervalo "1" equivale ao intervalo 01h00m00s à 01h59m59s e assim sucessivamente até o identificador de intervalo "23", que equivale ao intervalo 23h00m00s à 23h59m59s.

Em cada gráfico os resultados de vazão e perda de pacotes são apresentados de forma segmentada em relação aos protocolos de aplicação FTP, SSH, SMTP, HTTP e HTTPS, identificados a partir dos números de porta TCP: 21, 22, 25, 80 e 443, respectivamente. Em cada gráfico também foi apresentada uma série OUTROS que representa todas as demais portas TCP identificadas nos cálculos.

No dia 19 a vazão para os protocolos contidos na série OUTROS apresentou um comportamento atípico em relação aos demais dias analisados. Entre o intervalo de hora 0 e 21 a vazão ficou abaixo de 200 mil *bps*. Já no intervalo de hora 22 essa vazão sofreu uma ascensão repentina, ultrapassando 1 milhão de *bps*. Em seguida, no intervalo de hora 23 essa vazão foi zerada. O Gráfico 1 apresenta o comportamento da vazão no dia 19.

Obteve-se no dia 15 a maior porcentagem geral de perda de pacotes dentre os dias analisados. Nesse dia os protocolos HTTP, HTTPS e os contidos na série OUTROS sofreram as maiores perdas de pacotes dentre os dias analisados. O Gráfico 2 apresenta o comportamento da perda de pacotes no dia 15. Percebe-se no intervalo 8 desse gráfico uma queda brusca da perda de pacotes para os protocolos HTTP, HTTPS e os contidos na série OUTROS em relação aos intervalos anteriores.

ISSN: 1806-549X

Considerações finais

O presente trabalho permitiu extrair características a partir da vazão e perda de pacotes do tráfego de *internet* gerados nos laboratórios de informática do CCET.

Não foi objetivo deste trabalho realizar uma análise qualitativa do acesso à *internet* disponível para os laboratórios do CCET. Sendo assim sugere-se como um trabalho futuro a realização dessa análise com base em órgãos especializados. Propõe-se ainda como trabalhos futuros a interceptação do tráfego de *internet* integral da UNIMONTES por um período longo o suficiente que possibilite, com a medição do tráfego interceptado, a identificação de sazonalidades e a classificação das medições utilizando-se Redes Neurais Artificiais (RNAs) para que se conheça as classes existentes na rede de dados da UNIMONTES.

Agradecimentos

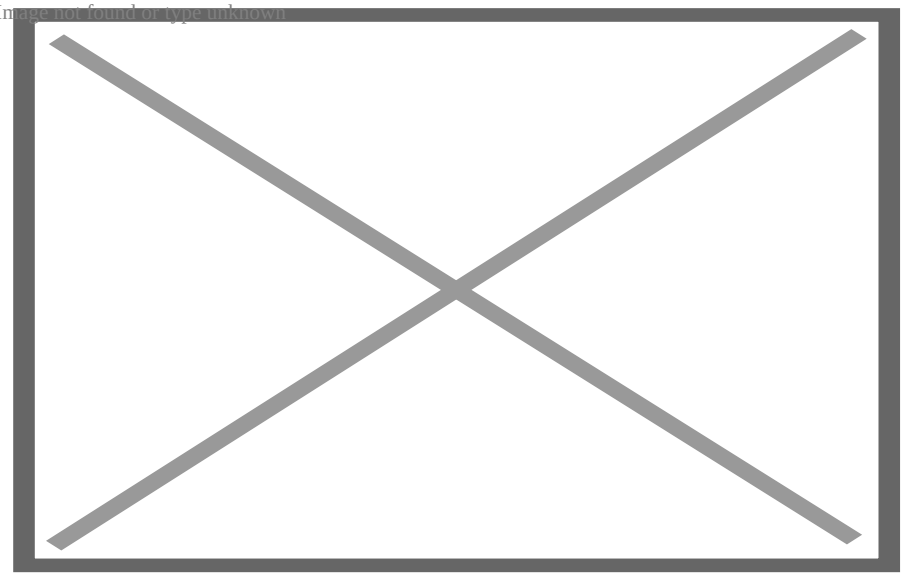
Agradeço ao Prof. Me. Allysson Steve Lacerda pelo empenho em fornecer significativas contribuições ao desenvolvimento deste trabalho. Agradeço ainda à FAPEMIG pelo financiamento da pesquisa.

Referências bibliográficas

[1] KUROSE, James F.; ROSS, Keith W.. **Redes de Computadores e a Internet**: uma nova abordagem. São Paulo: Pearson Addison Wesley, 2003. 530 p. Tradução de: Arlete Simille Marques.

[2] TEIXEIRA, Mauricio Santos. **Network Discovery**: Técnicas e Ferramentas. 2004. 46 f. Monografia (Especialização) - Curso de Administração em Redes Linux, Departamento de Ciência da Computação, Universidade Federal de Lavras, Lavras - MG, 2004. Disponível em: . Acesso em: 18 out. 2016.

Image not found or type unknown



ISSN: 1806-549X

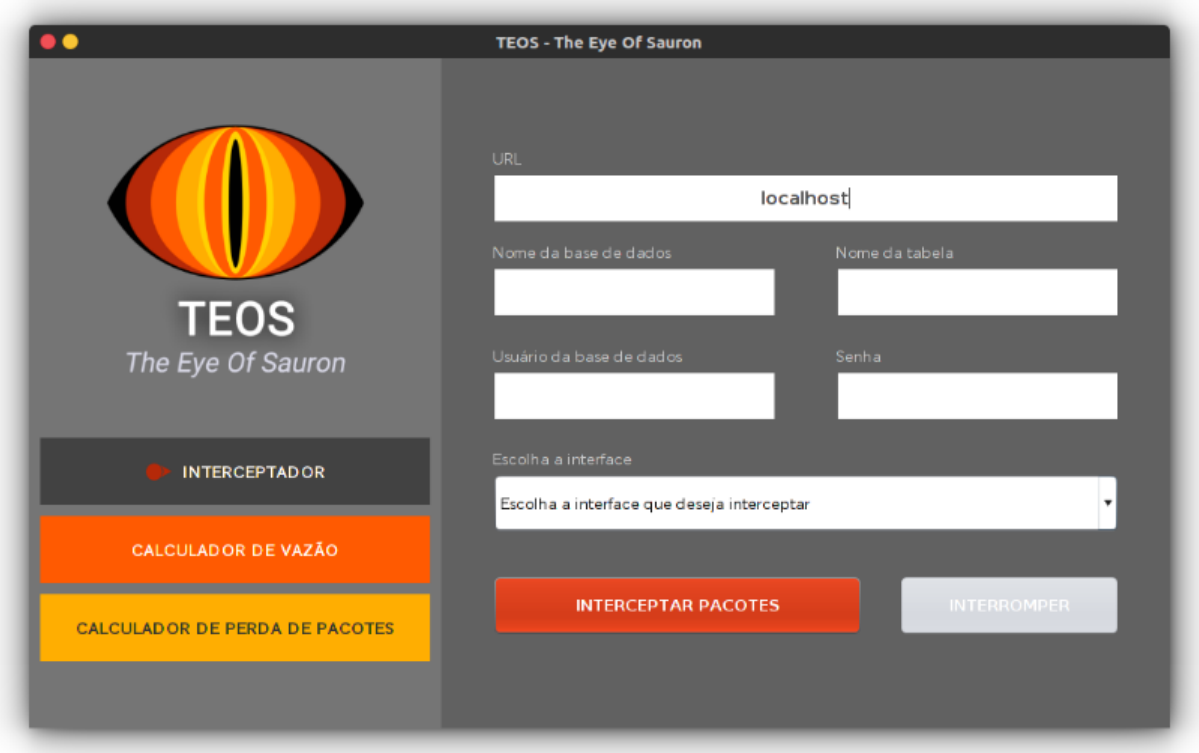


Figura 1. Interface do Sistema TEOS

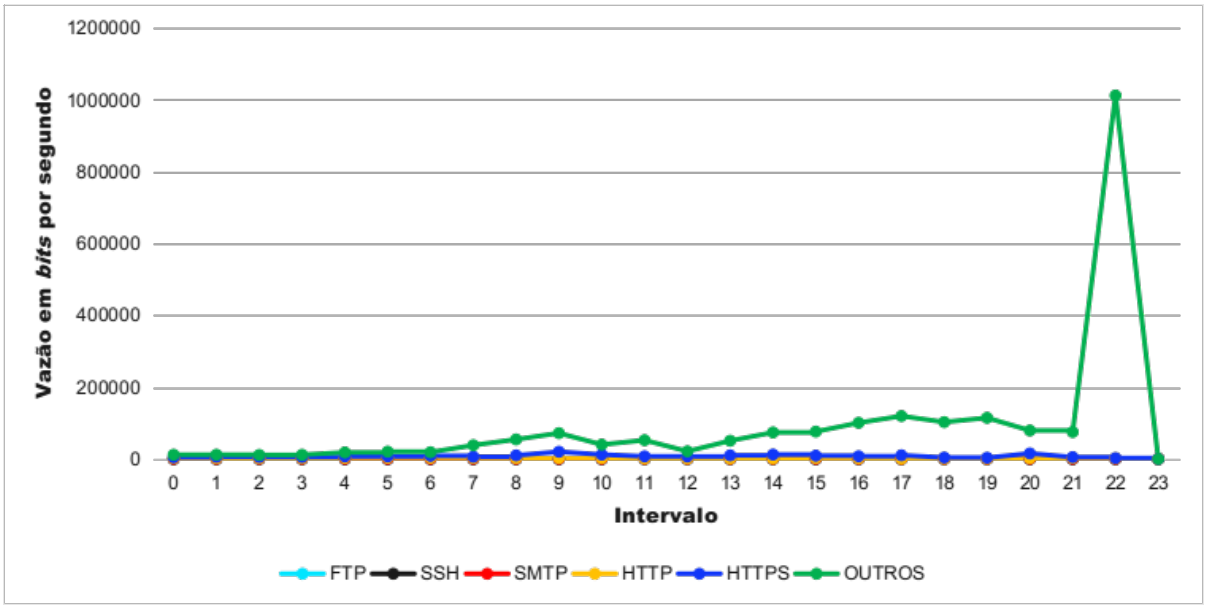


Gráfico 1. Vazão do dia 19 (quarta-feira)

ISSN: 1806-549X

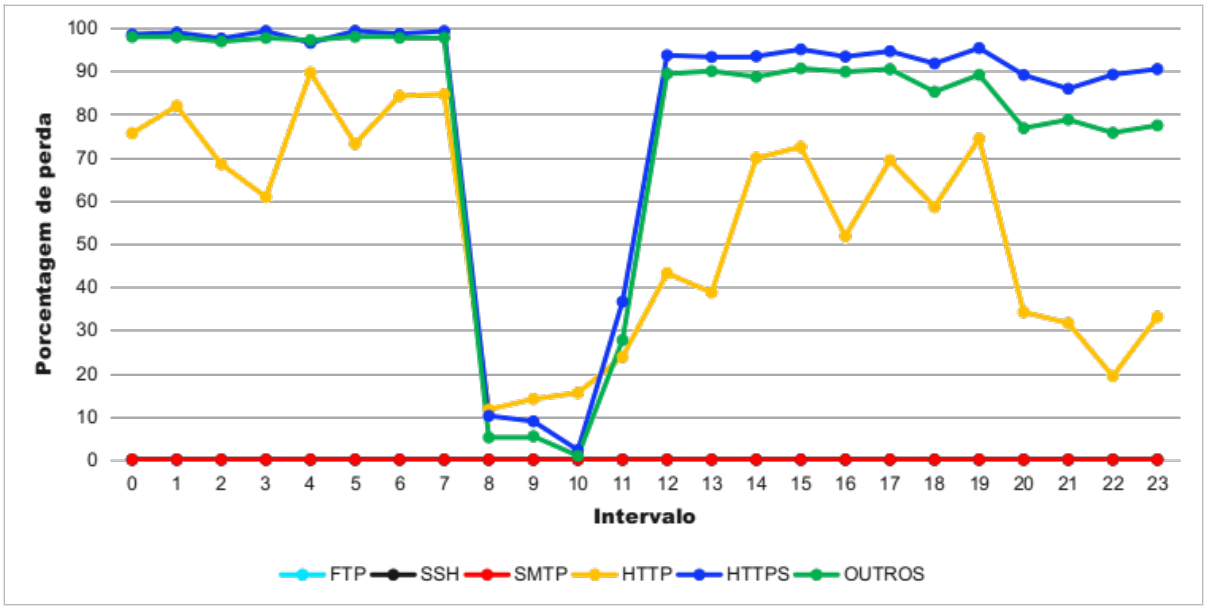


Gráfico 2. Perda de pacotes do dia 15 (sábado)