Relátorio de monitoramento de Redes

Bruno de Sena Pinheiro[1]

[1]Universidade Estadual do Ceará (UECE) – Centro de Ciência e Tecnologia
REDES DE COMPUTADORES

1. Introdução

O monitoramento de rede foi efetuado pelo programa ***wireshark*** em ambiente residencial, cujo acesso a rede de internet se dá por *WIFI*. O primeiro monitoramento ocorreu em período noturno com a utilização de filtro para observação apenas de pacotes de dados relacionados a conteúdo multimídia. Foi escolhido o *streaming* hospedado em **crunchyroll.com**, focado principalmente na visualização de vídeos de animações orientais. Para filtragem dos pacotes utilizou-se o filtro pelo ip **146.75.6.133** que estava responsável por distribuir os pacotes no momento do monitoramento. Em testes de monitoramentos anteriores ao que será apresentado neste documento observou-se que o ip responsável pela distribuição dos pacotes de dados multimídias relacionados ao conteúdo oferecido pelo *streaming* Crunchyroll mudava com o passar do dia. Dado interessante que deve estar relacionado à melhoria de acesso ao conteúdo de acordo com o volume de usuários(normalmente ocorrendo em horários específicos).

O segundo monitoramento apresentado neste documento concentrou-se na visualização de pacotes de dados relacionados a páginas da web. Optou-se por utilizar o filtro *tcp port 80 or tcp port 443* para que a observação se concentrasse no objeto escolhido através das portas para tráfego HTTP e HTTPS. Em ambos os monitoramentos o tempo de visualização ficou próximo de 1 hora e 5 minutos, destacando-se que o monitoramento de multimídia obteve um volume consideravelmente maior de pacotes em relação ao tráfego oriundo de páginas web, resultado já esperado devido a nátureza das informações em cada observação. Toda a análise dos datasets contendo a captura de dados foi efetuada com auxilio da aplicação *Jupyter Notebook* cujo código está disponibilizado no *github*.

1.1. Captura de tráfego multimídia

O arquivo CSV contendo o resultado do monitoramento de tráfego multimídia foi exportado com o nome *Captura de tráfego multimidia.csv*, contendo 3 427 252 pacotes de dados capturado em aproximadamente 3 925.88 segundos.

1.2. Captura de tráfego de dados

O arquivo CSV contendo o resultado do monitoramento de trafego pada dados de página web foi exportando com o nome *Captura de tráfego de dados.csv*, contendo 267 617 pacotes de dados capturados em aproximadamente 3 907.24 segundos.

2. Distribuição de Protocolos

Houve variação na quantidade de protocolos observados em cada uma das duas capturas efetuadas e, por isso, optou-se pela separação dos gráficos relacionados ao tráfego multimídia e ao trafego de dados de páginas web.

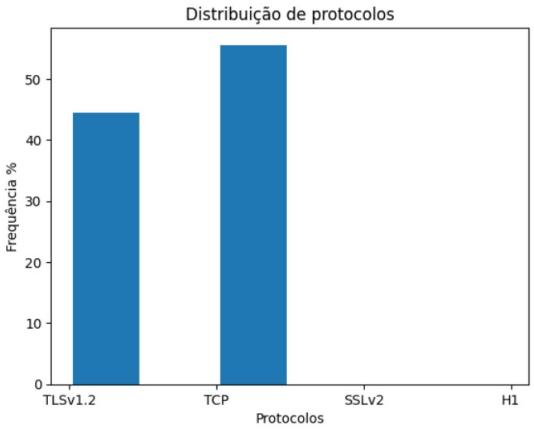

Figura 1. Distribuição de protocolos para tráfego multimídia.

Para o tráfedo de dados multimídias foram observados apenas os protocolos TLSv1.2, TCP, SSLv2 e H1 com uma forte predominância do TCP que possuia mais da metade dos pacotes. Os pacotes SSLv2 e H1 apresentaram um número tão baixo de pacotes que praticamente não aparecem no histograma. A tabela a seguir relaciona o valor total de pacotes para cada protocolo.

Distribuição de protocolos para tráfego multimídia

Protocolo	Quantidade de pacotes
TCP	1903724
TLSv1.2	1523509
SSLv2	17
H1	2

Os protocolos SSLv2 e H1 com respectivamente 17 e 2 pacotes observados não podem ser considerados relevantes no tráfego de dados multimídia observados na captura.

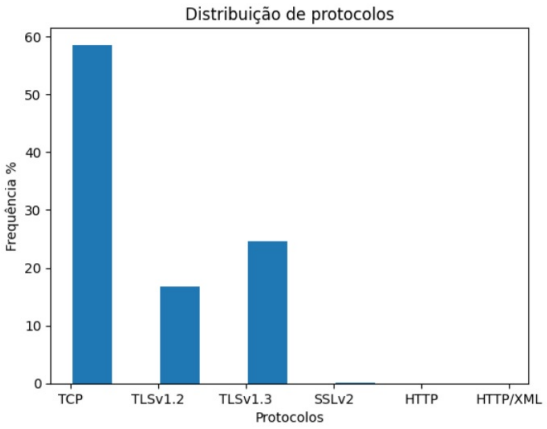

Figura 2. Distribuição de protocolos para tráfego em páginas web.

A figura 2 mostra que para o tráfego em páginas web há três protocolos relevantes, e destaca que apesar de não ser mais tão utilizado ainda é possível encontrar o protocolo HTTP em algumas páginas web.

Distribuição de protocolos para página web

Protocolo	Quantidade de pacotes
TCP	156712
TLSv1.2	44869
SSLv2	147
TLSv1.3	65807
HTTP	81
HTTP/XML	1

3. Largura de Banda

Para deretminação da largura de banda foi utilizado o somatório de todos os dados enviados por um IP específico em cada captura. Para o tráfego multimídia, devido ao filtro utilizado, apenas dois IPs enviaram informações pela rede: o **146.75.6.133** responsável pelos envios de pacotes do streaming Crunchyroll e o **192.168.0.104** que representa a máquina onde era efetuado o monitoramento.

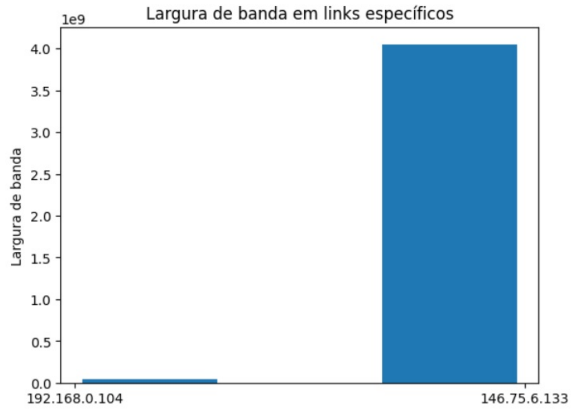

Figura 3. Largura de banda para tráfego multimídia.

Obviamente a largura de banda utilizada pelo link do streaming foi bem maior que a largura para a máquina de observação, tendo em vista que os pacotes enviados por **192.168.0.104** eram em sua maioria pedidos para o envio de pacotes multimídias (consideravelmente maiores) ampliando a banda de retorno para máquina.

No monitoramento da largura de banda para o tráfego em páginas web foram encontrados centenas de links distintos, optando-se por apresentar no gráfico apenas os 25 links mais relevantes da observação.

Os dois IPs mais relevantes observados são **68.67.153.38** e **192.168.0.104** que representam respectivamente uma distribuidora de dados para a empresa Meta (os pacotes estão ligados ao acesso a informações no site instagram.com) e a máquina responsável pela observação.

Largura de Banda para links mais relevantes

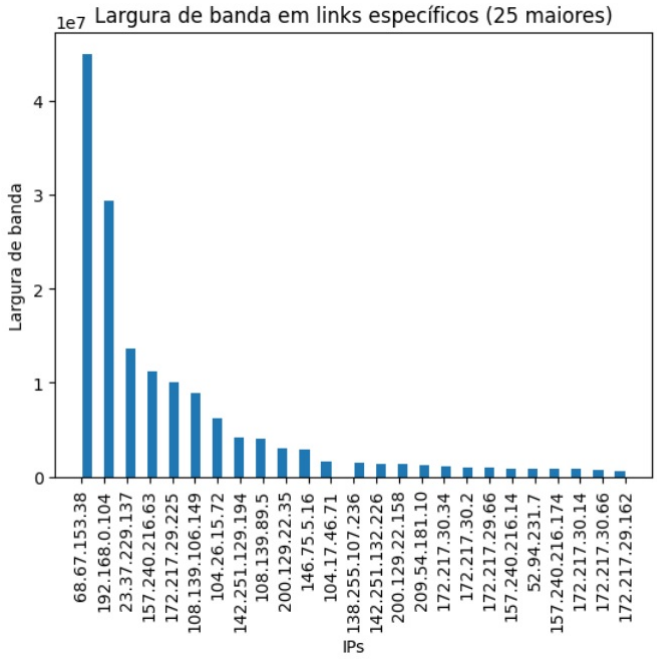

Figura 4. Largura de banda para tráfego em páginas web.

Link específico	Tráfego multimídia	Tráfego em página web
192.168.0.104	409555950	29299480
146.75.6.133	4052492809	
68.67.153.38		45014062
23.37.229.137		13601806
157.240.216.63		11171271
172.217.29.225		10030614
108.139.106.149		8839029
104.26.15.72		6208204
142.251.129.194		4171039
108.139.89.5		4043042
200.129.22.35		2977049
146.75.5.16		2947086

4. Volume de Tráfego

Como relação ao período de tempo, optou-se por utilizar o volume de tráfego por minuto, apresentado a informação em um gráfico de linhas conjuntas para facilitar a visualização. O volume total de dados para os tráfegos de dados multimídia e de páginas web foram respectivamente 4 093 448 404 e 176 230 705, mostrando como é bem maior o volume de dados para transmissão em streaming.

A linha representativa do tráfego para multimídia está normamente acima da linha que representa o tráfego para páginas web, mostrando apenas uma queda próximo ao período de 30 minutos que é visulamente inferior ao volume da linha vermelha nos primeiros minutos de observação. A queda se deu, provavelmente, devido a interrupção da transmissão.

Figura 5. Volume tráfego

5. Taxa de Pacotes Recebidos

A obtenção dos pacotes recebidos por segundo gerou um gráfico muito complexo para ser analisado em virtude das grandes variações e mais de 3900 cliclos de tempos apresentados. A taxa de pacotes multimídias recebidos é normalmente maior que a taxa de pacotes recebidos para dados de páginas web, mas em muitos segundos não é possível encontrar pacotes multimídias tendo sua taxa zerada nesses momentos.

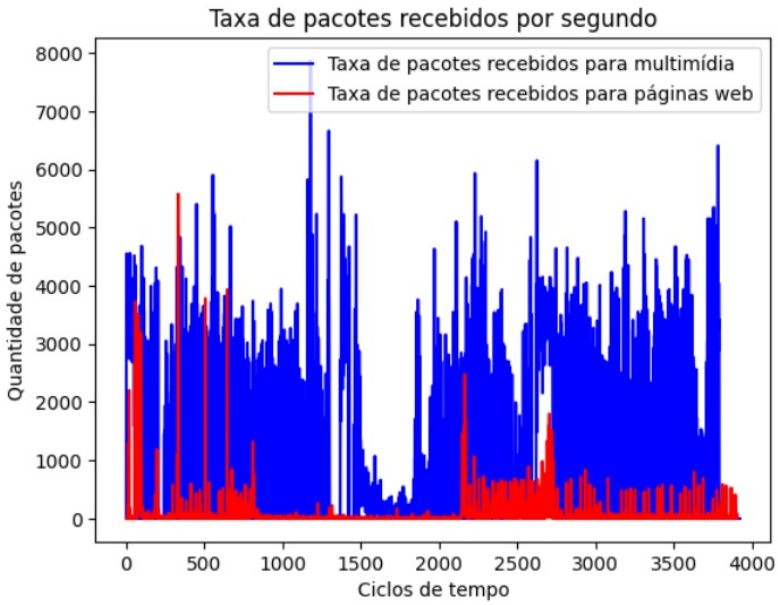

Figura 6. Taxa de Pacotes recebidos: linhas conjuntas

Para um melhor entendimento do gráfico, criou-se a opção de visualizar as taxa de pacotes recebidos em imagens separadas para cada monitoramento. As bases preenchidas nas figuras formadas nos gráficos mostram que em vários momentos não houve envio de pacotes. A altura do gráfico para transferência multimídia demonstra que há maior consumo de recurso de banda quando enviamos arquivos desse formato.

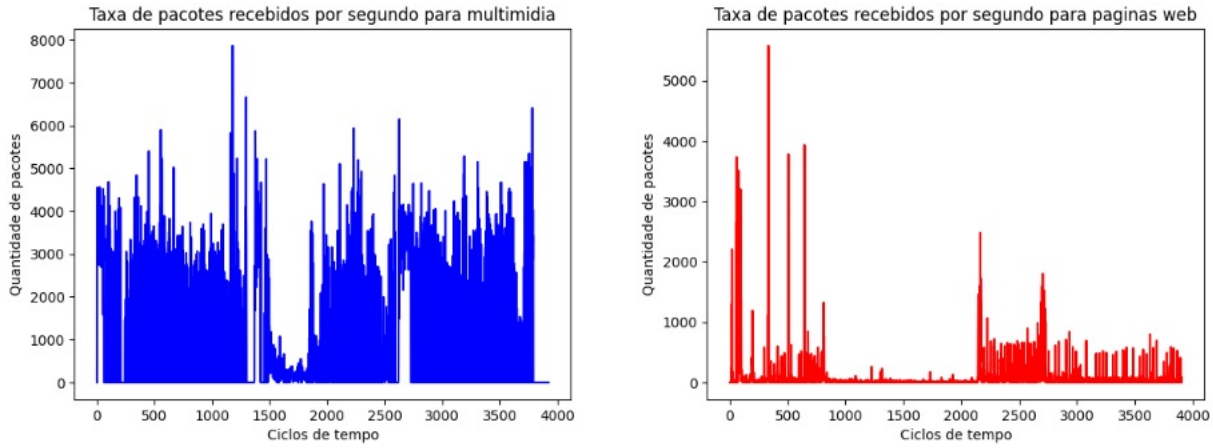

Figura 7. Taxa de Pacotes recebidos: linhas separadas

6. Conclusão

É evidente que o envio de informações multimídias pela rede demanda maiores recursos devido ao tamanho dos pacotes envolvidos na transmissão. Mesmo que algumas páginas web possuam elementos cujos downloads necessitam de pacotes maiores tal fato não é constante como ocorre em streaming. O monitoramento da rede se torna impressindível para determinar ações que proporcionem a melhoria do sistema e verificar quais atores são relevantes na tomada de decisam sobre como resolver futuros problemas relacionados ao envio e recebimento de dados.