IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

ARTIGOS

Detecção, análise e geolocalização de *middleboxes* presentes na *internet*

Por: Adenes Sabino Schwantz[1]

adenes.schwantz@ifc-videira.edu.br

Resumo

Esse artigo apresenta um estudo amplo e diversificado acerca da presença e influência de *middleboxes* na Internet nos dias atuais. Também é introduzida uma nova ferramenta, baseada no já existente Tracebox, capaz de detectar e geolocalizar *middleboxes* na Internet, campo que atualmente carece de uma ferramenta dedicada exclusivamente a esse propósito.

Palavras-Chave: Topologia da Rede; Descoberta; Monitoramento de Rede.

Resumo

Tiu artikolo prezentas larĝan kaj diversaj studo pri la ĉeesto kaj influo de middleboxes en Interreto nuntempe. Ĝi ankaŭ enkondukis novan ilon, bazita sur ekzistantaj Tracebox, kapabla detekti kaj geolocalizar middleboxes Interreto kampo nuntempe mankas ilo dediĉita ekskluzive al tiu celo.

Ŝlosilvortoj: *Reto topologio; Malkovro; Reto Monitoreco.*

Abstract

This paper presents a vast and diversified study about the presence and influence of middlebox appliance in nowadays Internet. A new tool is also presented here (based on Tracebox) which is capable of middlebox appliance detection and geolocation, a field which needs a dedicated tool to fulfill this demand.

Keywords: *Network Topology; Network Discovery; Monitoring Network; Topology; Network Discovery; Monitoring.*

1. É especializando em Automação Industrial, é graduado em Engenharia Elétrica pelo Instituto Federal Sul-Rio-Grandense - IFSUL e pela *Queen Mary University of London* e é Técnico em Eletrônica pelo Centro Federal de Educação Tecnológica de Pelotas/ RS. É servidor público federal, docente EBTT, lotado na cidade de Videira/ SC.

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

INTRODUÇÃO

Redes de computadores modernas fazem uso, em sua grande maioria, da já consolidada arquitetura TCP/IP, arquitetura esta projetada para obedecer o princípio *End-To-End*. Este princípio define que em uma rede de propósito geral, aplicações de fim específicos devem residir em *hosts* na borda da rede, e não em nós intermediários, dessa forma adquirindo confiabilidade de diferentes partes componentes da rede (SALTZER *et al*., 1981).

Sendo assim, em uma hierarquia clássica, assume-se que a rede contém *hosts* implementando as camadas de transporte e aplicação, roteadores implementando a camada de rede e processando pacotes, etc.

Entretanto, redes modernas, especialmente as mais recentes, não respeitam mais este princípio. Grandes redes corporativas, pontos de *WiFi* e, especialmente, redes celulares frequentemente incluem vários diferentes tipos de *middleboxes* (SHERRY *et al*., 2012). Em sua definição, *middlebox* nada mais é do que "qualquer aparelho intermediário desempenhando funções diferentes das normais ou roteamento de pacotes entre uma fonte e um destino, sendo assim manipulando tráfego com funções diferentes de roteamento."(WANG *et al*., 2011).

Já é passada a hora de se construir um conhecimento mais sólido acerca dessas *middleboxes*, suas funções mais comuns, onde estão presentes e de que forma atuam. Sua presença já é uma realidade e precisamos lidar, cedo ou tarde, com sua interferência que, em certos momentos, pode ser até mesmo descontrolada.

É notoriamente sabido que *middleboxes* são difíceis e complexas de se lidar, no caso da rede, e de detectar, no caso do usuário comum. Existe uma grande falta de ferramentas dedicadas a esse propósito. Recentemente uma nova ferramenta foi proposta e validada, e chamada, por seus autores, de a evolução do *traceroute* (DETAL *et al*., 2012). Esta ferramenta, *Tracebox*, permite a detecção de quais *middleboxes* modificam pacotes em praticamente qualquer caminho de rede. Este artigo propõe uma extensão ao

Tracebox, permitindo um acesso consideravelmente mais fácil à ferramenta. Também, além de apenas fornecer o IP da *middlebox*, determinar e fornecer a localização dessa *middlebox*, exibindo a localização de todas as *middleboxes* detectadas em um mapa, e isso tudo com fácil e amplo acesso, apenas necessitando-se de conexão à Internet e um *web browser*.

Por fim, um estudo acerca da presença de *middleboxes*, e de seus comportamentos em diferentes situações com diferentes tipos de tráfego, é apresentado. Essa associação de uma ferramenta de fácil acesso e manipulação com um estudo dedicado visa trazer mais conhecimento sobre esse problema cada vez mais presente nas redes do século XXI.

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

MIDDLEBOXES

Cabe aqui uma breve discussão sobre *middleboxes*, visto que estas são o grande objeto de estudo deste artigo. Como já definidas anteriormente, pode ser classificado como *middlebox* qualquer dispositivo da rede que executa funções além de roteamento de pacotes. Estes dispositivos são frequentemente usados por questões de segurança e desempenho. Típicas *middleboxes* incluem NATs (*Network Address Translators*), *firewalls*, DPIs (*Deep Packet Inspectors*), *proxies* transparentes, sistemas de detecção e prevenção de intrusos, etc.

Essas *middleboxes* devem ser em teoria totalmente transparentes para o usuário final, porém diversas experiências mostram que as mesmas possuem um impacto negativo na evolução do protocolo TCP/IP (HONDA et al., 2011).

Isso só mostra a importância que estes dispositivos têm e que não podem mais serem tratados com pouca importância.

TRACEBOX

A extensão desenvolvida e o estudo baseado na mesma tem como base uma complexa e ampla ferramenta desenvolvida para detectar *middleboxes*, o Tracebox.

O Tracebox usa de um mecanismo similar ao *traceroute* (JACOBSON et al., 1989) para detecção de *middleboxes* ao longo de um caminho. Os pacotes enviados são inspecionados no retorno a fim de detectar qualquer modificação que possam ter sofrido por conta de uma *middlebox*. O Tracebox permite ao usuário o controle dos pacotes a serem enviados (Cabeçalho IP, Cabeçalho TCP ou UDP, Opções TCP, carga, etc.). Ele possui o recurso de manter ambos pacotes, o original enviado e o pacote de retorno, sendo assim

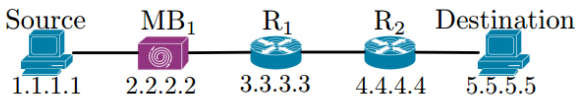
possível detectar modificações.

Outro recurso importante é o fornecimento do IP da *middlebox* em que ocorreu a modificação, que proporciona a possibilidade da geolocalização da mesma.

A seguir será descrito sucintamente o funcionamento do Tracebox, sendo que o mesmo é uma ferramenta base do estudo feito e exposto aqui, para uma ampla análise e validação da ferramenta o artigo "Revealing Middlebox Interference with Tracebox" (DETAL et al. 2011) deverá ser consultado.

Em síntese, Tracebox funciona em duas etapas: detecção e prova. Na primeira, detecção, envia pacotes incrementando

seus TTLs iterativamente, até atingir o host de destino. Nesta fase é possível identificar roteadores que respeitam a RFC1812, ou seja, que retornam dentro do pacote ICMP todo o pacote (no caso o pacote enviado pelo Tracebox) que teve seu TTL expirado. Na segunda, prova, permite a comparação do pacote original enviado com o pacote retornado, sendo possível assim identificar possíveis modificações sofridas pelo pacote retornado.



(a) Topologia

```
# tracebox -p 'IP / TCP / mss(9000)' -n 5.5.5.5
tracebox to 5.5.5.5 (5.5.5.5): 30 hops max
1: 3.3.3.3 TCP::SequenceNumber
2: 4.4.4.4 IP::TTL IP::CheckSum TCP::CheckSum TCP::SequenceNumber
           TCPOptionMaxSegSize::MaxSegSize
3: 5.5.5.5
```

(b) Saída

Figura 1 – Exemplo do Tracebox (DETAL et al., 2012)

Na figura 1(a) uma rede simples é mostrada, onde MB1 é uma *middlebox* que modifica o número de sequência TCP. Na figura 1(b) pode ser vista a saída do Tracebox. Podemos ver que a MB1 é efetivamente identificada, porém isso ocorre um salto acima do esperado, visto que o roteador R1 é um roteador antigo e não respeita a RFC1812. O roteador R2 é um roteador novo, respeitando as RFCs mais recentes, portanto "citando" em sua resposta todo o pacote expirado. Dessa forma o Tracebox apenas detecta a modificação um salto acima. Isso nos mostra o quão importante é termos o equipamento de rede atualizado respeitando as mais recentes RFCs. Também concluí-se que num futuro próximo, com equipamentos mais recentes, o Tracebox será capaz de identificar

com sucesso toda e qualquer *middlebox* em determinado caminho.

O TTL e o IP *checksum* são modificados em cada roteador e a modificação no TCP *checksum* resulta das modificações no cabeçalho TCP.

Vemos que em casos pontuais como o exemplificado aqui, o Tracebox não identifica a localização da *middlebox* precisamente, porém, na grande maioria dos casos essa *middlebox* se encontra na mesma rede local do roteador (R1) e com isso sua localização é confiável.

Tracebox ainda possui outras funcionalidades como a capacidade de definir pacotes personalizados e execução de *scripts*. Ambas as opções dão um grande poder à ferramenta e serão utilizadas, nessa e em versões futuras, da extensão da

ferramenta abordada aqui.

TRACEBOX VISUAL

Nesta seção expõe-se a justificativa de um aprimoramento à ferramenta já apresentada aqui. O Tracebox é uma excelente ferramenta realizando a sua proposta de detecção de *middleboxes*. Porém ainda é uma ferramenta restrita e não está amplamente difundida. Existem alguns motivos que podem ser apontados como razões do retardo de sua difusão. Entre eles o difícil acesso à ferramenta, fora do meio acadêmico e, mais especificamente, dos pesquisadores ligados à área a ferramenta não é conhecida, o que leva ao desconhecimento da mesma por grandes clientes em potencial, como grandes empresas de telecomunicações, por exemplo.

Outra razão, nesse caso voltando o pensamento à usuários puntuais, é sua difícil integração com o sistema operacional. Primeiramente somente se encontra disponível para usuários do sistema Linux e MAC OS X, excluindo a plataforma Windows e plataformas móveis (Android, iOS). Segundo, possui difícil instalação, requerendo conhecimento avançado e instalação de diversos pacotes de *softwares* auxiliares.

Por último, se trata de uma ferramenta avançada sem um manual à sua altura. Excluindo a função básica de enviar um pacote padrão a um destino, o Tracebox torna-se difícil de manipular. A especificação de um pacote pode se tornar algo complexo, devido à estrita sintaxe de comandos e parâmetros que devem ou não ser omitidos.

Sua saída nos fornece os IPs das *middleboxes*, mas não temos ideia alguma de como estas estão distribuídos entre fonte e destino, se se concentram nas bordas ou no *backbone* da rede.

Com isto em mente, se percebe que há espaços para melhorias. Sendo assim, uma ferramenta simples e efetiva, além de dinâmica e acessível foi projetada e desenvolvida, tendo em mente a ideia primária de acesso simplificado e universal, surgindo o Tracebox Visual.

O Tracebox Visual tem em seu núcleo o Tracebox clássico, que está hospedado em um servidor Linux remoto. Com simples acesso à Internet e um *web browser* é possível ter acesso ao mesmo, sem necessidade de qualquer instalação adicional. Um conjunto de informações básicas acerca da ferramenta é oferecido ao usuário, bem como opções de especificação de pacotes e um conjunto

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

de exemplos de como utilizá-los. Toda documentação e apresentação já existentes também são oferecidas. Exemplos de saída esperada e um guia de instalação da ferramenta no próprio sistema do usuário também é parte integrante do *website*.

Por fim, como não poderia deixar de ser, todo o conteúdo do Visual Tracebox é oferecido nos idiomas português e inglês, inicialmente. Fomentando assim sua utilização ao redor do globo.

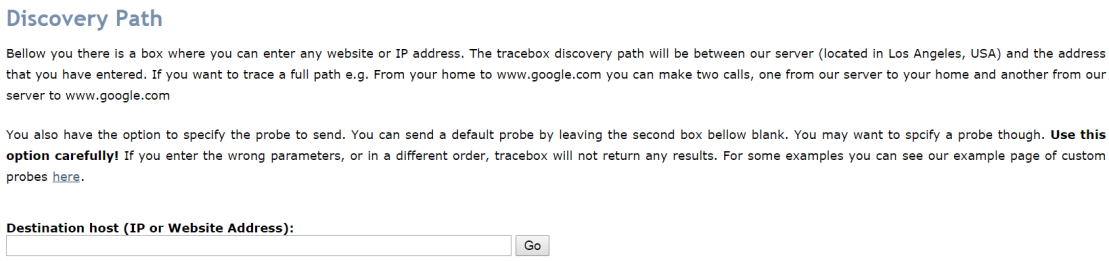


Figura 2 – Interface para inserção do endereço de destino do caminho, pelo usuário. (Elaborado Pelo Autor)

Na Figura 2 acima vemos uma seção ampliada do *website*, onde o usuário deve entrar com endereço IP ou *website* que desejar para realização a detecção de *middleboxes* e posterior geolocalização das mesmas.

Assim que o usuário entrar com o endereço e clicar no botão designado, o processo do Tracebox é iniciado no servidor, com os parâmetros fornecidos. Com uma seleção dos IPs das *middleboxes* detectadas no caminho, é feita a geolocalização através de uma API dedicada a este fim. IPs com coordenadas válidas são pinados no mapa e o caminho por onde a informação passou é mostrado. Tudo isso de forma simples e objetiva. A saída em modo texto que o Tracebox fornece também é exibida, afim do usuário poder identificar os tipos de *middleboxes* encontradas.

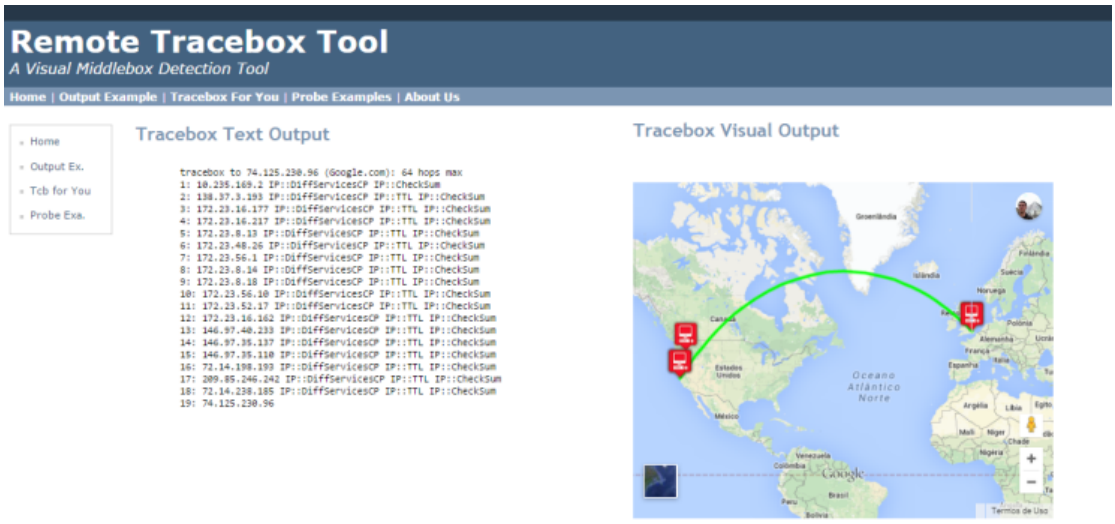


Figura 3 – Saída fornecida ao usuário. (Elaborado Pelo Autor)

Como pode ser visto na figura 3, o resultado é oferecido ao usuário da forma mais clara possível. Para o exemplo apresentado está sendo mostrado um processo do Tracebox disparado de Londres em direção ao endereço www.google.com, foram

detectadas 18 *middleboxes* alterando o campo DiffServices. Várias dessas *middleboxes* se encontram próximas, sendo assim no mapa pode-se ver (com auxilio da ferramenta de *zoom*) cerca de quatro locais diferentes.

Ainda há aspectos a evoluir, e mais características importantes a oferecer ao usuário dessa ferramenta. Este tópico será apresentado na seção trabalhos futuros.

O Visual Tracebox, para detecção visual de *middleboxes*, em sua versão alfa, a atual, se encontra disponível para uso restrito atualmente. Nessa versão ainda estão sendo realizados testes, portando falhas ainda desconhecidas podem ocorrer. A capacidade atual, por se tratar de uma ferramenta gratuita utilizando somente processos e APIs gratuitos, é de um usuário por vez e 50000 acessos diários. Até sua versão final essas questões serão tratadas a fim de obter uma acessibilidade de mais qualidade.

MIDDLEBOXES: UM ESTUDO DE CASO

Com o Visual Tracebox (e remoto) funcionando sem grandes problemas e ainda sem um estudo aprofundado acerca de *middleboxes* usando esta ou outra ferramenta semelhante, uma ideia válida surge, a de estudar-se, ao menos em parte, efeitos, localizações e presença de *middleboxes* na Internet em geral.

a) Experimento I: Resultados e Discussão

O primeiro experimento proposto tratou de enviar um pacote pré-definido para uma lista de *websites* usando dois modos de conexão: Ethernet versus HSDPA. O pacote usado consiste de um pacote padrão TCP/IP com algumas opções TCP importantes. A especificação do pacote, em linha de comando, é dada por:

IP/TCP/MSS/MPCAPABLE/TS/SACKP/WSCALE/NOP

O grupo estudado se trata de uma mescla de *websites* do Alexa's top 5000 de *websites* mais acessados no mundo com endereços de diferentes servidores e de diferentes classes (A, B e C) IP.

Alguns aspectos importantes foram levantados. Certas modificações repetitivas foram identificadas, a primeira delas, no campo TTL (*time to live*) era esperada, já que um pacote deve ter esse campo decrementado a cada salto, para evitar que o pacote circule indefinidamente na rede. Teve-se também uma modificação recorrente no IP *checksum*. Considerando um pacote TCP/IP, sabe-se que o *checksum* de dados (usado para verificação de erro) não inclui o campo TTL, assim pôde-se concluir que ao longo do caminho entre origem e destino, em praticamente todos os caminhos testados existem *middleboxes*. Porém nesse caso, não foi possível obter-se mais detalhes acerca das mesmas, visto que essas *middleboxes* também desfaziam suas modificações, assim apenas identificou-se que uma alteração ocorreu, visto que o *checksum* foi alterado. Isso pode indicar a presença de NATs, pois os mesmos alteram os endereços de destino dos pacotes na entrada e desfazem essa modificação na saída de suas redes. Não se pode

esquecer que o TTL e o IP *checksum* são modificados em cada roteador, portanto o que indica a efetiva presença de uma *middlebox* é a modificação no TCP *checksum* resultante de (in)determinada alteração no cabeçalho TCP.

Atendo-se a esta última modificação causada por *middleboxes* no TCP *Checksum* do pacote pode-se concluir que, na grande maioria dos casos, ocorreu juntamente com modificações nas opções adicionadas ao pacote. Mesmo não havendo outras modificações expostas abertamente no mesmo salto. A conclusão para ocorrência dessa anomalia é de que o roteador (ou outro dispositivo de rede) que retornou essa modificação não é subordinado à RFC 1812.

São necessárias certas considerações sobre RFCs (*Request for Comments*), a fim de demonstrar a constatação feita aqui. Existem duas importantes RFCs que tratam de mensagens de resposta ICMP, do mesmo tipo usado pelo Tracebox. A primeira, digna de menção no caso, é a RFC792, que diz que o roteador onde o campo TTL atingiu o valor 0 deve incluir apenas o cabeçalho IP do pacote em sua resposta. Já a RFC1812, mais recente e que revoga a RFC792, especifica que o roteador deve incluir todo o pacote IP em sua resposta de TTL 0 (*time exceeded*).

Com isso, conclui-se que na Internet, mesmo em seu *backbone*, seus dispositivos ainda não obedecem a, pelo menos, uma das RFCs a que estão submetidos, e, portanto ainda enviam respostas incompletas, o que pode afetar usuários e dispositivos nas mais

diversas formas. Nesse caso não se esperava essa constatação importante, porém foi obtida graças ao aspecto da ferramenta Tracebox que trabalha com ICMP e que necessita de um pacote-resposta ICMP que obedeça a RFC 1812 para uma análise mais eficaz das *middleboxes*, como explicado anteriormente. Ainda na questão da modificação no cabeçalho TCP conclui-se assim que não é possível usar pacotes deste tipo confiavelmente como assinatura de uma *middlebox*.

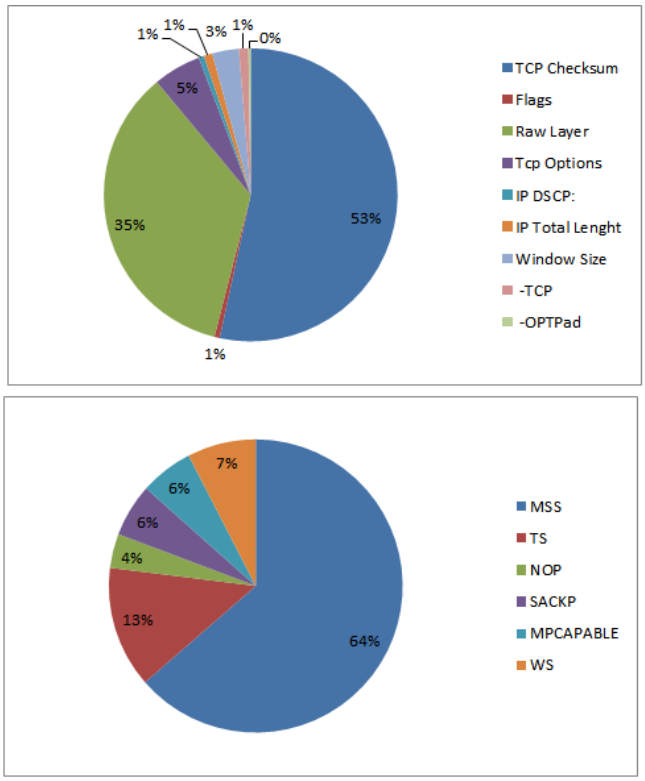
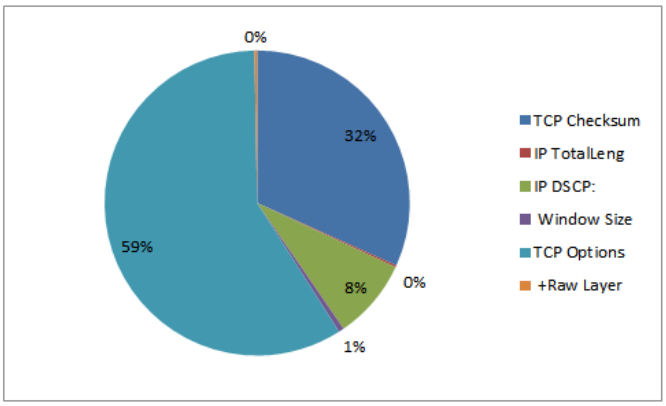


Figura 4 – Distribuição das modificações detectadas na conexão Ethernet. (Elaborado Pelo Autor)

A figura acima mostra os resultados obtidos na conexão Ethernet. O gráfico superior inclui todas as modificações encontradas, nos cabeçalhos e nas opções. O gráfico inferior mostra somente as opções TCP modificadas e suas proporções.

A próxima figura obedece ao mesmo critério. Gráfico superior exibindo o resultado geral das modificações encontradas, seja nos cabeçalhos TCP e/ou IP, seja nas opções manualmente adicionadas ao pacote. Enquanto isso, no gráfico inferior, é mostrada a proporção de modificações ocorridas nas opções, tão e somente. Logicamente esses resultados agora representam as modificações e resultados pertinentes à conexão 3G.



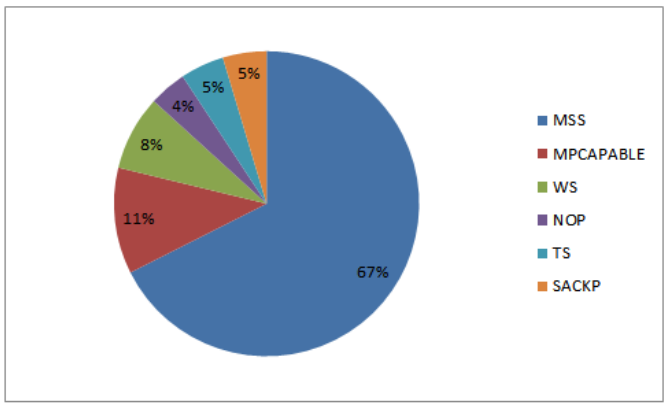


Figura 5 – Distribuição das modificações detectadas na conexão 3G. (Elaborado Pelo Autor)

Percebem-se claramente diferenças entre os modos de conexão analisados. Uma das mais importantes a ser destacada é a quantidade de modificações do TCP *checksum* na conexão cabeada, representado mais da metade do total. Esta é a primeira prova de que existiram modificações detectadas pelo Tracebox, porém sobre as quais não foi possível obter mais detalhes. Isso é reflexo da diminuta quantidade de roteadores que obedecem a RFC1812, provando que os equipamentos de rede presentes ainda não respeitam as RFCs mais atuais. Por outro lado vemos que na rede 3G, mais nova e atualizada, essa quantidade cai para cerca de 30%, provando que a mesma atende aos requisitos impostos pelas RFCs de maneira mais eficaz.

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

A prova de que existe uma quantidade significativa de *middleboxes* nas redes celulares vem do fato de que as modificações nas opções TCP chegam a 65%. Outro fato importante é o aumento significativo das modificações no valor de IP DSCP em comparação com a conexão cabeada.

Numa análise geral dois aspectos importantes já foram destacados, porém deve-se prestar atenção especial em algumas opções. Uma das conclusões importantes adquiridas a partir desta experiência é sobre as mudanças no Máximo Tamanho do Segmento (MSS). Depois de alguns testes realizados, antes do experimento, notou-se que algumas *middleboxes* alteram o valor MSS, sempre para 1380 bytes. O valor padrão do Tracebox para MSS é maior do que isso, o que é útil para detectar comportamentos diferenciados da rede. Os resultados foram, de certo modo, surpreendentes, visto que em ambos os modos de conexão a alteração de valor do MSS representa mais do que 60% do total de modificações das opções.

O valor mínimo do MSS para IPv4 é de 534 bytes e para IPv6 1280 bytes. Basicamente esta opção especifica a maior quantidade de dados que o *host* pode receber em um único segmento TCP. O datagrama IP contendo o segmento TCP pode estar auto-contido dentro de um único pacote, ou pode ser reconstruído a partir de várias partes fragmentadas. De qualquer forma, o limite de MSS aplica-se a quantidade total dos dados contidos no segmento TCP final, ou reconstruído. Para a maioria dos usuários, o valor da opção de MSS é estabelecido pelo sistema operacional.

Essa questão ainda esta em aberto, mesmo após pesquisa, pois não há como ter certeza do por que essa mudança está ocorrendo com tanta frequência. Porém o objetivo principal, de detectar *middleboxes* realizando modificações nessa opção, foi alcançado. Futuramente um estudo relacionado à descoberta de caminho MTU pode ser realizado, visto que a conexão TCP deve checar essa opção durante essa descoberta. Infelizmente os pacotes usados nesse experimento não são capazes de testar essa situação.

Outro aspecto que merece ser detalhado é o DSCP IP. Este campo não parece ter muita importância para conexão cabeada, mas é totalmente diferente para a rede 3G. Este campo foi modificado oito vezes mais na rede 3G, às vezes isoladamente e às vezes juntamente com opções TCP. Analisando essas modificações, nota-se que, por padrão, o valor foi ajustado para 10, sendo

que o valor padrão é zero. Aparentemente, o campo DSCP é usado pela rede para fins de classificação, que está intimamente relacionada com o fator Qualidade de Serviço (QoS).

A conclusão é que a *middlebox* altera esse valor tentando melhorar a QoS para a transmissão do pacote. A maioria das mudanças DSCP ocorreu perto do destino, o que leva a crer que se trata de uma política de rede que da preferência a certos pacotes sobre outros. Ainda há a possibilidade do uso combinado do fator QoS com MPLS, porém isso requer um estudo futuro dedicado à essa situação, visando confirmação.

b) Exeperimento II: Resultados e Discussão

O experimento II foi focado em *websites* específicos de três continentes, a fim de avaliar possíveis diferenças entre os mesmos e diferenças geográficas. Trata-se de um experimento menos robusto que o primeiro, e engloba as regiões da Ásia, Europa e América. A metodologia de levantamento dos resultados foi similar à anterior. Os resultados variaram consideravelmente de região para região. As diferenças entre os tipos de conexão mantiveram as mesmas características.

Os principais dados levantados foram importantes na compreensão das diferentes implementações da rede em cada região. Para a região da Ásia, um alto índice de remoção de opções e alteração de valores foi detectado, possivelmente indicando uma alta, e descontrolada, presença de *middleboxes*. Para a Europa, obteve-se o menor índice de alterações, com praticamente 90% dos

caminhos sem importante presença de *middleboxes*. Por fim um caso inesperado, no continente americano uma grande quantidade de modificações foi detectada próximo ao destino. Estudos preliminares indicam uso de QoS (Qualidade de Serviço), comportamento somente observado nesse continente, durante todos os experimentos.

c) Experimento III: Resultados e Discussão

Por último, chega-se ao experimento III. Neste experimento diversos destinos do Alexa's top 100 foram analisados. Também foi utilizado o modo de conexão 802.11, de forma a identificar possíveis diferenças, também esse tipo de conexão pôde ser usado para uma comparação com os dados do experimento I. Obviamente que usando 802.11 poderia se esperar ter diferenças significativas apenas nos primeiros saltos.

Alguns dos resultados mais importantes e merecem ênfase são a rejeição de pacotes com a opção *Multipath* (multi-caminho), recentemente implementada. Também houve uma ainda maior rejeição da opção MSS nesse experimento.

A ideia aqui foi de comparar esses endereços, que estão dentre os mais acessados no mundo, com os endereços do experimento I, e analisar assim se há diferenças importantes entre redes com grande trafego de dados e redes com menos tráfego, e usando um conjunto de diferentes pacotes (especificados) para teste. A princípio não houve uma grande diferença, como esperado, e a suposição inicial foi confirmada. Novamente pacotes-padrão não sofreram tantas modificações tanto quanto aqueles com opções adicionadas e outras variações.

Novamente a rede HSDPA (3G), mais recente, obedece as mais recentes RFCs, pois usam equipamento mais novo, sendo assim mais modificações foram observadas e detectadas.

Por último, cabe citar a mais importante constatação feita e confirmada com este experimento. Não foi apenas uma anomalia, mas um fato, de que as redes 802.11 não aceitam largamente a nova opção de *multipath*. A remoção dessa opção contribui com 14% das modificações encontradas em redes 802.11, enquanto em redes HSDPA esse valor gira em torno de apenas 1%.

É fato conhecido que essa recente extensão, *multipath* TCP, ao protocolo inclui um complexo mecanismo, que constitui a maior parte do protocolo, exclusivamente para lidar com *middleboxes*. Ainda assim, vemos um índice considerável de rejeição a esta nova opção.

Contribuições

Com esta série de experimentos conduzida, resultados coletados e analisados acredita-se ser possível obter mais conhecimento e se conhecer mais detalhes acerca das *middleboxes* operando na Internet ao redor do planeta. Diferentes modos de conexão foram abordados e o conhecimento de suas particularidades em relação ao assunto em questão pode ser agora expandido.

O resultado final, somada uma análise, proporciona a expansão desse conhecimento específico na área, além de indicar algumas novas direções a se seguir, como por exemplo, a reação esperada e a detectada em relação ao *Multipath* TCP.

Em relação ao Visual Tracebox ainda não há dados concretos, pois a ferramenta ainda está em fase de testes e é desconhecida do público. Porém espera-se que se torne mais popular, graças ao fácil e simples acesso, ajudando com isso a se

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

construir mais conhecimento em relação à *middleboxes* e inclusive o fomento da ferramenta Tracebox, seja por usuários isolados, corporações ou instituições de ensino e pesquisa.

Trabalhos Futuros

A ferramenta apresentada ainda encontra-se em sua versão inicial e com o tempo sua funcionalidade será incrementada com recursos já previstos e com outros podendo vir de sugestões de usuários. Dentre acréscimos a serem feitos em versões futuras, já se pode citar suporte a *scripts*, onde o usuário poderá submeter rotinas próprias a serem executadas. Mais detalhes acerca da *middlebox* detectada também serão fornecidos junto da interface gráfica, em forma de balão, bastando o usuário clicar no local apontado no mapa para obter essas informações extras. Novos e diferentes estudos também poderão ser feitos pelos autores da ferramenta ou usuários da mesma.

Conclusão

Muito mudou na Internet desde seu começo. Uma solução, inicialmente, nos dias atuais se tornou um problema: o espalhamento sem controle de *middleboxes*. Neste artigo uma série de experimentos conduzidos foi apresentada, a fim de se

ampliar o conhecimento sobre as mesmas. Importantes características, como presença e modificações realizadas, foram obtidas, e tudo isso feito com uma boa abrangência ao redor do globo.

Uma nova ferramenta também foi introduzida, o Visual Tracebox, ferramenta esta que possibilita o fácil acesso ao estudo em geral ou específico direcionado à *middleboxes*. Tudo gratuitamente e de fácil acesso, sem necessidade de profundos conhecimentos específicos.

Com isso, espera-se ampliar o conhecimento, elucidar os problemas relacionados e desenvolver soluções em diferentes níveis de rede, envolvendo *middleboxes*.

IΦ-*Sophia*

Revista eletrônica de investigação filosófica, científica e tecnológica

REFERÊNCIAS

SALTZER, J. H.; REED D. P.; CLARK D. D. "End-to-End Arguments in System Design". *In*: **International Conference On Distributed Computer Systems**, v. 2 n. 101, p. 509-512, 1981.

SHERRY J.; HASAN S.; SCOTT C.; KRISHNAMURTHY A.; RATNASAMY S.; SEKAR V. "Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service". *In*: **Proc. ACM SIGCOMM Conference**, v. 18 n. 85 p. 13-24, 2012.

WANG Z.; QUIAN Z.; XU Q.; MAO Z.; ZHANG M. "An Untold Story of Middleboxes in Cellular Networks," *In*: **Proc. ACM SIGCOMM Conference**, v. 17 n.44 p. 374-385, 2011.

JACOBSON V. "Traceroute" *In*: UNIX, man page, n. 3, Janeiro de 1989, Disponível em: ftp://ftp.ee.lbl.gov/traceroute.tar.gz (source Code). Acesso em 12.05.2016

DETAL G.; HESMANS B.; BONAVENTURE O.; VANAUBEL Y.; DONNET B. "Revealing Middlebox Interference with Tracebox" *In*: **Proc. ACM SIGCOMM Conference**, v. 18 n. 85 p. 1-8, 2012.

HONDA M.; NISHIDA Y.; RAICIU C.; GREENHALGH A.; HANDLEY M.; TOKUDA H. "Is It Still Possible to Extend TCP" *In*: **Proc. ACM SIGCOMM Conference**, v. 17 n. 13 p. 181-194, 2011.