Sonata: Query-Driven Streaming Network Telemetry

Grupo 1
Francisco Caeiro, **47823**
Bruno Andrade, **47829**
António Estriga, **47839**

Qual é o problema que os autores tentam resolver?

Nos sistemas atuais de telemetria, existe uma separação entre a recolha de dados e a configuração (parametrização) da análise dos dados recolhidos. Esta separação faz com que este processo seja lento e de elevado custo. Estes sistemas fazem uma recolha de dados (*headers*, *size*, *IPs*, *ports*. etc.) e uma análise posterior relativo ao tráfico na rede para razões de segurança ou de gestão do uso da própria rede.

Os autores tentam assim arranjar um algoritmo que faça uso da análise para realizar uma melhor configuração à recolha dos dados, por outras palavras, em vez do processo ser feito num único sentido passa a ser feito em ambos.

Este problema é relevante?

A análise e monitorização do tráfico da rede são cada vez mais importantes, visto que é através dela que se realiza trocas de informação, utilização de recursos ou serviços. Ao analisarmos o tráfico na rede, e os respetivos pacotes, podemos ainda, através dos seus parâmetros, detetar certos ataques informáticos.

Qual é a sua solução? Que novas técnicas foram usadas?

A solução foi criar o Sonata, um sistema de telemetria que suporta uma interface para novos tipos de queries (unificadas, particionadas, dinâmicas), arquitetado de maneira modular e extensível, ao mesmo tempo que refina as queries dinamicamente para serem usadas em recolhas de tráfico posteriores.

O sistema é dividido em dois componentes, o processador de *stream* de dados e o controlador *runtime*. O processador de *stream* trata de receber os dados ou metadados (pacotes, tuplos) enviados pelos *switches*, que são os resultados das queries feitas. O processador é responsável pela análise da informação recebida e é este que decide e ajusta as queries necessárias para a próxima análise. Por outro lado, o controlador *runtime* é responsável por transformar e enviar o conjunto de *queries* para os *switches.*

As *queries* podem ser realizadas através de uma abstração de linguagem, sendo "traduzidas" para linguagens do *data plane* (P4) e, comunicando com os *switches*, possamos obter pacotes ou tuplos relativos aos dados desejados. Isto permite que o utilizador, que programa o controlador, não se tenha de preocupar com estes detalhes. Estas queries são expressas como se fossem operações de *dataflow*.

As queries podem ser particionadas utilizando os dispositivos programáveis existentes na rede, que podem executar um subconjunto de operações no *data plane*, reduzindo número de pacotes e tuplos à custa de guardar estado na rede. São operações para um *data plane* baseado em PISA, que permite novos campos nos cabeçalhos, suportar um estado simples de computação, funções de *hash* personalizável e tabelas de *match/action* mais flexíveis, por outras palavras, permite funções de *map, filter, sample, join*, entre outras.

A última técnica é o uso de *queries* dinâmicas ou feitas iterativamente, que, como foi explicado previamente, são queries que são ajustadas à medida que se recolhem mais dados. Este ajuste é feito através da análise dos dados recolhidos anteriormente, aumentando o nível de granularidade de certos subconjuntos ou em certas janelas temporais. Isto, por usa vez, causa uma perda no poder de processamento de pacotes e o custo de manter o estado do *data plane*.

Como é que se destaca de trabalhos anteriores?

Uma das principais diferenciações de trabalhos anteriores, ou até mesmo tecnologia anterior, é o facto que existe um ajuste dinâmico e semiautomático das *queries* a serem enviadas e processadas pelos *switches*. Até à data de publicação do artigo, as *queries* eram feitas à base de palpites, estimando que, num intervalo de tempo dado, estas dessem alguma informação útil sobre o estado da rede. No entanto, como a recolha deriva da análise anterior, as *queries* são ajustadas da melhor forma que o sistema prevê.

Quais são os pontos mais fortes deste artigo? E os seus pontos fracos?

Como um dos pontos mais fortes é, sem dúvida, a novidade na área de telemetria que permite o uso da análise para se poder recolher dados mais detalhados sobre o estado da rede. Este artigo pode vir a ser a base nos quais os futuros sistemas de telemetria se baseiem.

Um dos pontos fracos do artigo é que este explica conceitos que, à primeira vista, são simples mas, assim que se entra no detalhe dos mesmos, tendem a ser bastante complicados, o que pode levar a uma perda no raciocínio lógico e explicativo do artigo.

Como nota final, é de notar que os autores partilharam publicamente o Sonata, facilitando a contribuição para novos e melhores sistemas ou serviços da área.

Como seria uma extensão deste trabalho?

Um dos problemas do sistema desenvolvido é não tratar de conflitos de *queries* no *data plane* antes do *runtime*. Este seria um dos problemas a resolver utilizando, por exemplo, outros artigos que já resolvem este problema noutras situações. Outra ideia seria fazer um artigo na perspetiva do utilizador deste sistema para perceber melhor os seus defeitos e virtudes.