Evento	Salão UFRGS 2020: SIC - XXXII SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2020
Local	Virtual
Título	Biblioteca de features para monitoramento de fluxos
Autor	MATHEUS SAUERESSIG
Orientador	ALBERTO EGON SCHAEFFER FILHO

Título: Biblioteca de features para monitoramento de fluxos
Autor: Matheus Saueressig
Orientador: Alberto Egon Schaeffer-Filho
Instituição: UFRGS

Desenvolvida na linguagem P4 (Programming Protocol-Independent Packet Processor), o repositório P4Features se propõe a ser uma biblioteca modular, simples e de acesso universal a ferramentas de captação de informações da rede chamadas features. Atualmente existem diversos trabalhos envolvendo monitoramento de redes em linguagem P4, seja para desenvolver soluções de segurança ou de otimização para um servidor. Embora esses trabalhos utilizem métricas em comum, os códigos são estruturados de maneira que gera dificuldade a transposição da captação dessas métricas para outras soluções. P4Features é uma biblioteca que busca poupar o trabalho do desenvolvedor, ofertando actions declaradas de forma modular, para que possam ser utilizadas para diversos fins, bem como facilitar sua transposição e reutilização em outros trabalhos. A biblioteca é estruturada como sendo um conjunto de actions, um equivalente às funções de outras linguagens, onde as métricas como contadores de bytes e de pacotes são salvas em registradores. Cada índice de um registrador representa um fluxo de rede diferente. Por exemplo, um registrador que conta bytes chamado byte_cnt_reg, possui n índices, indicando que há n fluxos de rede sendo monitorados. Em cada índice, está a quantidade de bytes de cada fluxo. Atualmente, a biblioteca conta 6 features. Planejamos ampliar continuamente a biblioteca, adicionando features mais complexas e especializadas, mas sempre prezando pela modularidade e fácil acesso a elas. Como caso de uso, P4Features está sendo utilizada em trabalhos de pesquisa da UFRGS, como um projeto de floresta aleatória com propósito de detectar possíveis ataques de negação de serviço (DoS) e um sistema para coleta de snapshots de rede.