Uma ferramenta para avaliação de algoritmos de classificação de anomalias para tráfego Internet

Anderson Santos da Silva, Juliano Araujo Wickboldt, Alberto Schaeffer-Filho, Angelos K. Marnerides, Andreas Mauthe
Instituto de Informática, Universidade do Rio Grande do Sul, Brasil
Email: {assilva, jwickboldt, alberto}@inf.ufrgs.br
School of Computing and Communications, Lancaster University, United Kingdom
Email: {a.marnerides2, a.mauthe}@lancaster.ac.uk

Resiliência e redes de computadores

- Resiliência é a capacidade da rede de manter níveis aceitáveis de operação frente a anomalias, como sobrecarga operacional ou problemas de configuração.
- A classificação de tráfego é uma estratégia frequentemente utilizada como mecanismo de detecção de anomalias no contexto de redes resilientes.
- Algoritmos de *Machine Learning* podem ser utilizados para classificação de tráfego da Internet

PReSET e detecção de anomalias

- A ferramenta PReSET (Policy-driven Resilience Strategy Evaluation Toolset) foi desenvolvida para permitir a simulação de estratégias de resiliência orientadas a políticas. Ela suporta a avaliação de estratégias que são expressas utilizando a linguagem de especificação de políticas Ponder2.
- Um classificador de tráfego Internet foi desenvolvido sobre a ferramenta PreSET com o intuito de prover detecção de tráfego malicioso na rede. A arquitetura do sistema é ilustrada na figura 1

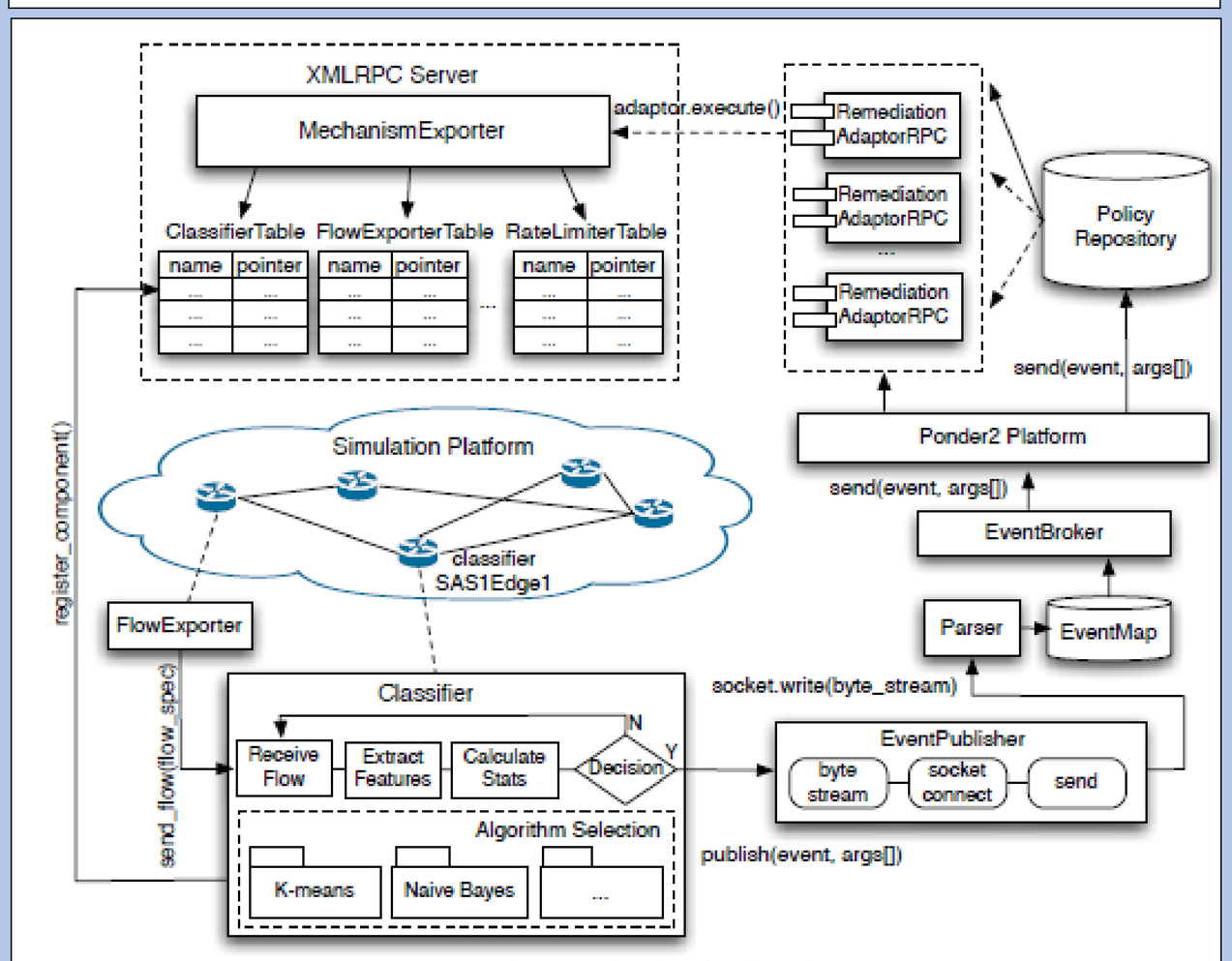
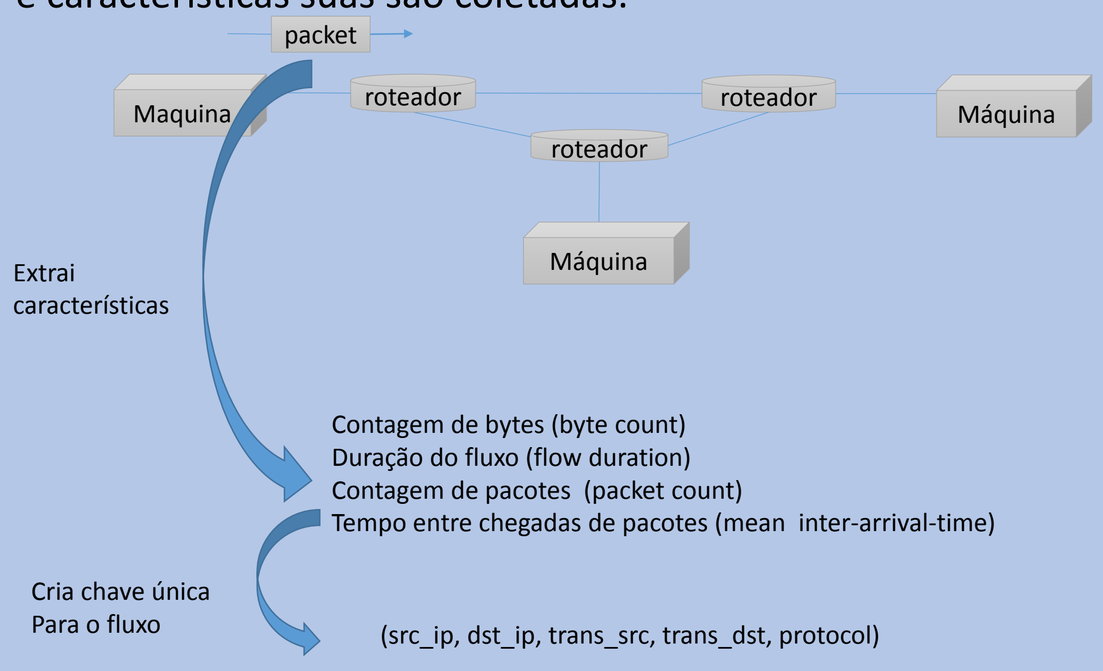


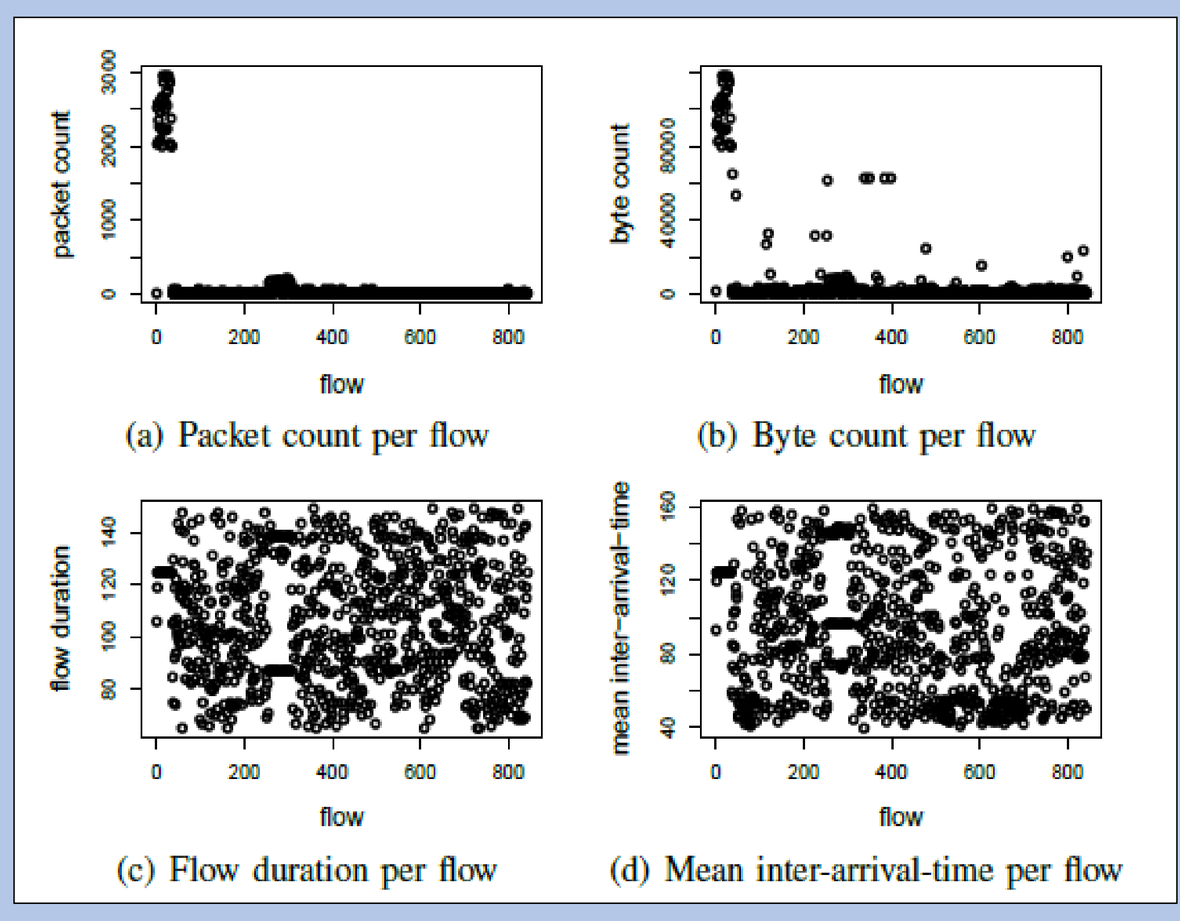
Fig 1 – Arquitetura do nosso classificador de tráfego

- Passo 1: Cada fluxo na rede é interceptado por nosso classificador e características suas são coletadas.

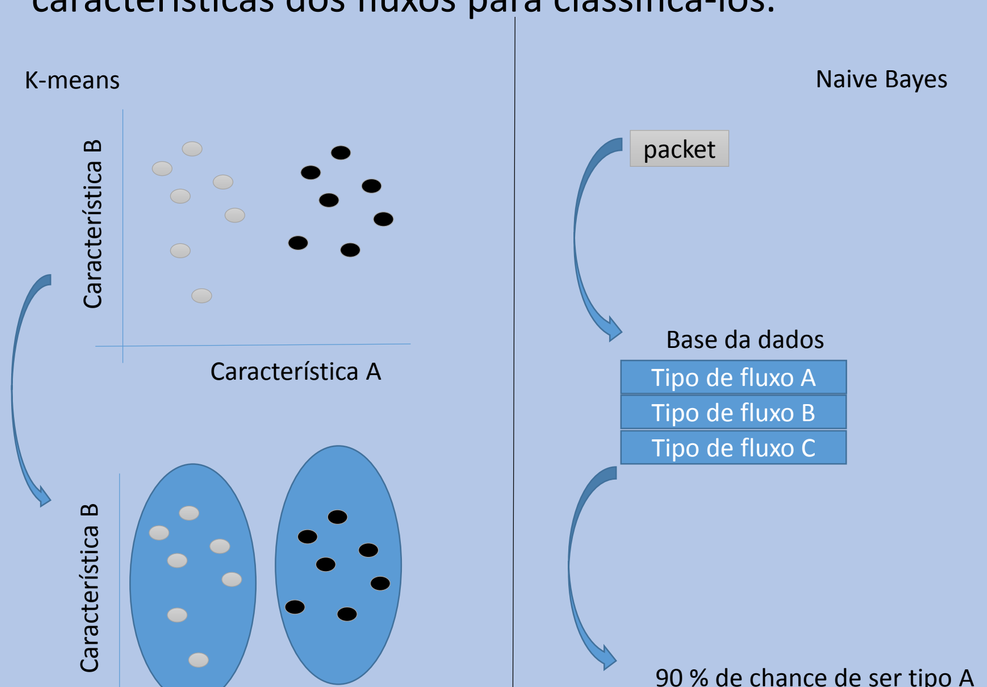


Processo de Classificação

- Passo 2: As características com distribuições mais homogêneas foram escolhidas para representar os fluxos na rede



- Passo 3: k-means e Naïve Bayes foram utilizados sobre as características dos fluxos para classificá-los.



- Passo 4: Cada fluxo é classificado e rotinas de mitigação podem ser acionadas para bloquear fluxos maliciosos