Deteção de acesso a plataformas de streaming

Técnicas de Percepção de Redes

Grupo:
João Oliveira 93295
Miguel Fernandes 93284

Problema de Segurança

Acesso a plataformas de streaming que são estritamente proibidas dentro de uma empresa.

Certos departamentos de uma empresa não devem ter acesso a plataformas de streaming pois afeta a produtividade visto que são atividades de lazer. Então é importante detetar esses acessos ilícitos.

O acesso a plataformas de streaming menos fidedignas pode comprometer a segurança do departamento de uma empresa bem como a própria empresa como um todo.

Problema de Segurança

Com base nos comportamentos de tráfego corretos dos diferentes departamentos, pretende-se detetar desvios - problema de anomalia.

Implementação

Considera-se uma empresa dividida em 3 departamentos:

- Recursos Humanos;
- Finanças;
- Desenvolvimento de software.

Através do tshark obtiveram-se capturas durante 20 minutos nos diferentes departamentos para representar um comportamento normal em cada um:

```
$ tshark -i wlo1 -w fin.pcap 'src host 192.168.1.190 and dst net 0.0.0.0/0'
```

Recursos Humanos: YouTube, mails PDFs, videoconferência, upload e download de vídeos e PDFs, notícias, Facebook e Linkedin.

Finanças: upload e download de PDFs, mails, acesso ao site das Finanças e Segurança Social.

Desenvolvimento de software: Pesquisas variadas, upload e download no GitHub.

Observação

Janelas de 60 segundos com deslocamentos de 10 segundos com as métricas:

- Número de pacotes de download e upload;
- Número de bytes de download e upload.

Features:

- Time independent: média, mediana, desvio padrão, assimetria e percentis(75,90,95 e 98);
- Time dependent: média e desvio padrão dos períodos de silêncio e períodos de atividade.

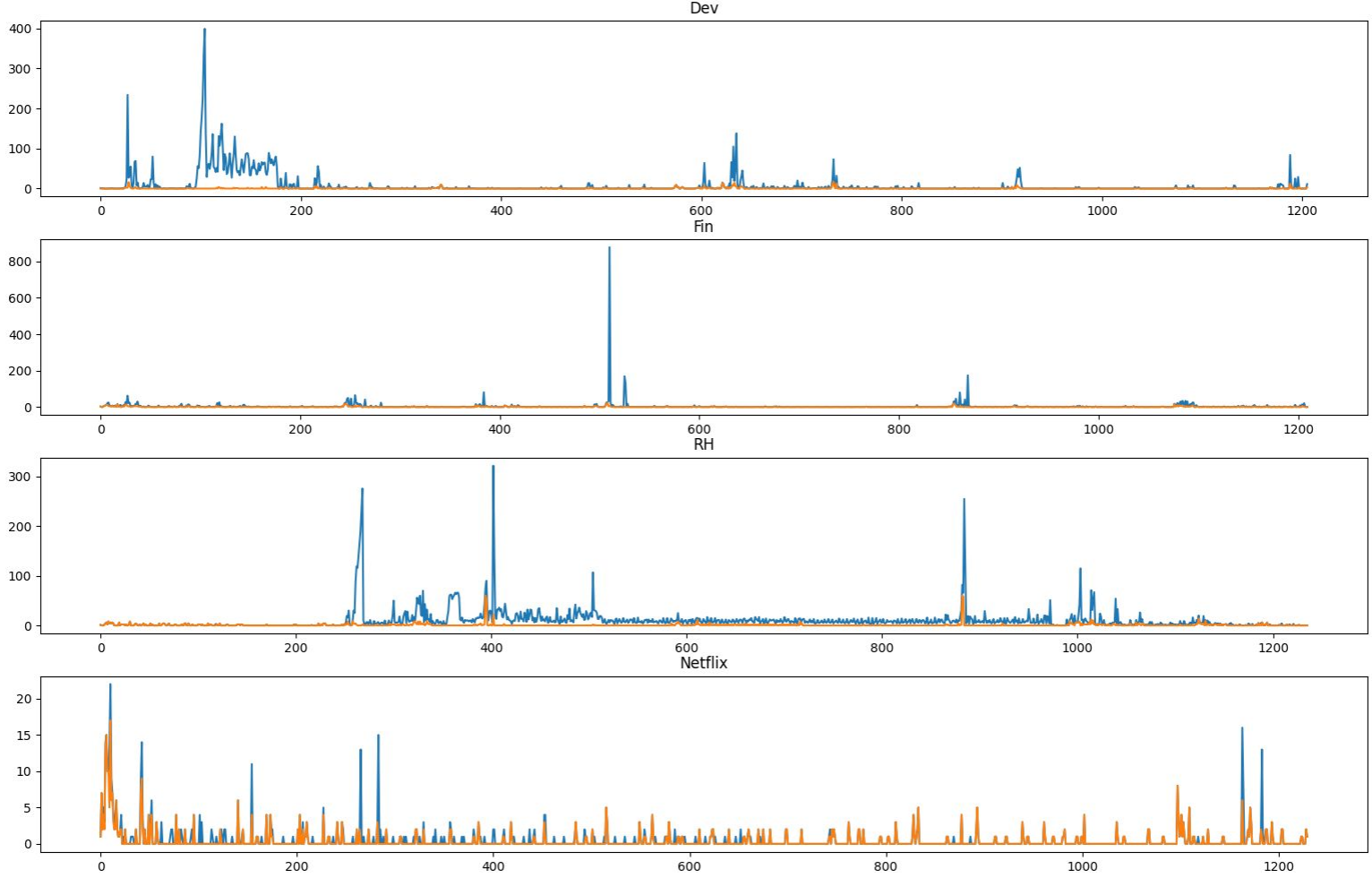

Fig 1. Download e Upload de Pacotes

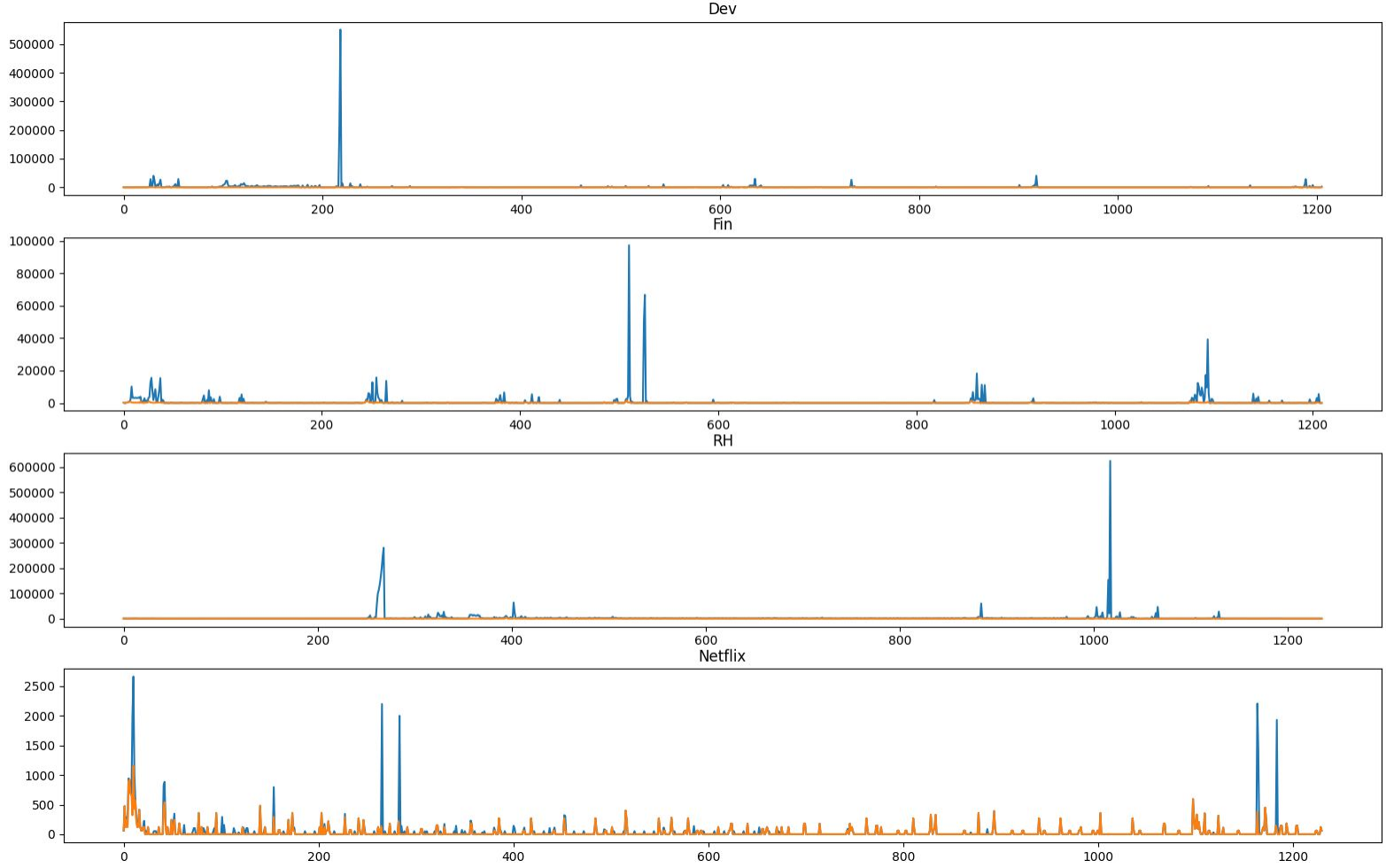

Fig 2. Download e Upload de Bytes

Deteção de Anomalias

Considerámos o tráfego Dev, Fin e RH como bom e o tráfego Netflix como anomalia.

Usámos OneClass-SVM com kernels linear, RBF e polinomial para detetar anomalias.

```
-- Anomaly Detection based on One Class Support Vector Machines (PCA Features) --
Dev Anomaly
Kernel Linear:  68.42105263157895 %
Kernel RBF:  42.10526315789473 %
Kernel Poly:  70.17543859649122 %
Dev Anomaly = 12.280701754385964 %

Fin Anomaly
Kernel Linear:  68.42105263157895 %
Kernel RBF:  29.82456140350877 %
Kernel Poly:  54.385964912280706 %
Fin Anomaly = 1.7543859649122806 %

Rh Anomaly
Kernel Linear:  52.54237288135594 %
Kernel RBF:  37.28813559322034 %
Kernel Poly:  72.88135593220339 %
RH Anomaly = 1.694915254237288 %
```

```
-- Anomaly Detection based on One Class Support Vector Machines --
Dev Anomaly
Kernel Linear:  47.368421052631575 %
Kernel RBF:  73.68421052631578 %
Kernel Poly:  47.368421052631575 %
Dev Anomaly = 31.57894736842105 %

Fin Anomaly
Kernel Linear:  47.368421052631575 %
Kernel RBF:  54.385964912280706 %
Kernel Poly:  47.368421052631575 %
Fin Anomaly = 7.017543859649122 %

Rh Anomaly
Kernel Linear:  54.23728813559322 %
Kernel RBF:  49.152542372881356 %
Kernel Poly:  57.6271186440678 %
RH Anomaly = 22.033898305084744 %
```

Conclusão

Sem PCA, com Linear e Poly obtivemos resultados semelhantes e mais satisfatórios do que com RBF.

Com PCA concluímos que com o RBF se obtiveram os melhores resultados

No geral concluímos que com PCA os resultados obtidos foram bastante melhores.