Percepção da utilização da rede na biblioteca da UA

Henrique Silva 88857
Pedro Silva 89228

Técnicas de Percepção de Redes

Problema

Classificar padrões dos utilizadores da rede da biblioteca da UA:

- Estudo (leitura de artigos)
- Entretenimento (streaming)
- Aulas online
- P2P (ilícito)

Bloquear conteúdo ilícito após a sua deteção:

- P2P

Detectar anomalias(bots):

- Intervalos periódicos entre pedidos

Data Sources

Uso de máquinas virtuais para simular os pedidos à rede.

Captura de pacotes no dispositivo pessoal conectado à rede da UA.

Used datasets and metrics to extract from raw data

Pacotes capturados com Wireshark durante cerca de 70 minutos.

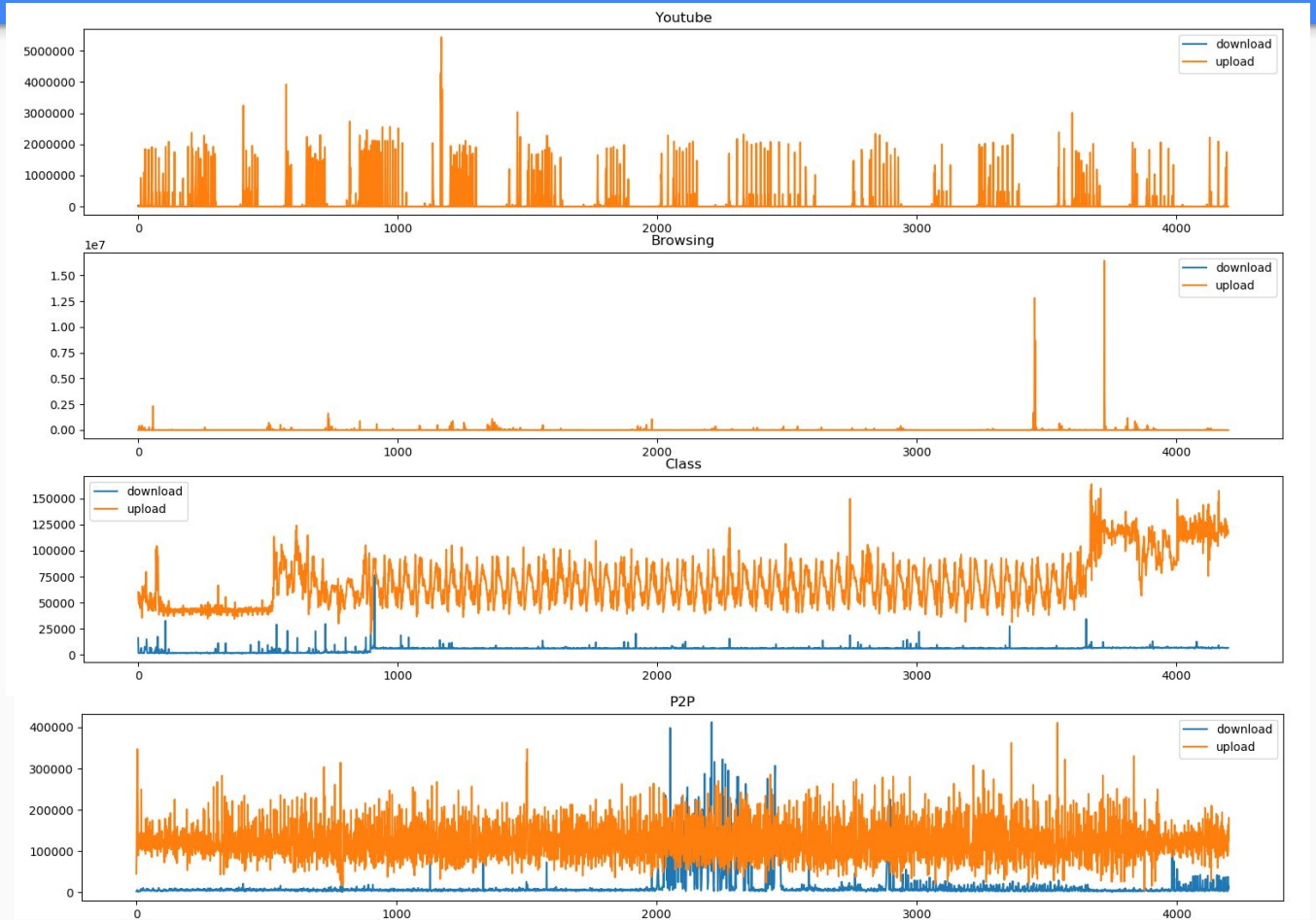
Pacotes de diferentes atividades:

- Browsing (notícias e artigos)
- Youtube com reprodução automática
- Vídeo chamada no Microsoft Teams
- µTorrent com download/upload limitado a 112 kb
- Comportamento de 3 diferentes bots (para a deteção de anomalias)

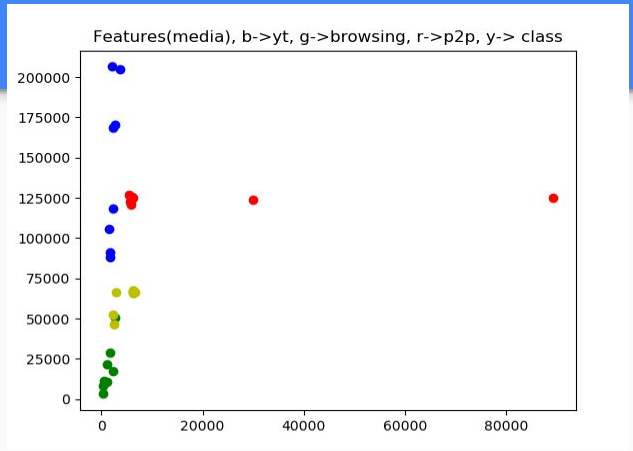
Processamento dos pacotes extraídos para a obtenção do número de downloaded bytes/uploaded bytes em cada segundo.

Armazenamento num ficheiro de texto.

Packets metrics



Deteção de Anomalias



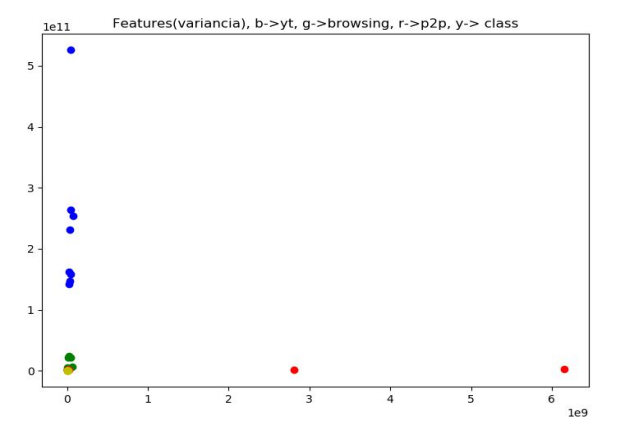
Features utilizadas:

- Variância
- Média
- Média e desvio padrão do silêncio (threshold 256 bytes)
- Wavelets

Modelos de Machine Learning:

- One Class Support Vector Machines (permite detectar o outsider num conjunto de dados)
  - com e sem PCA features
  - função linear, rbf (radial basis function) e polinomial

Samples de 5 minutos
Percentagem treino - 60%
Percentagem teste - 40%



Resultados

One Class Support Vector Machines (PCA Features):

- Kernel Linear - 63%
- Kernel RBF- 70%
- Kernel Poly- 60%

One Class Support Vector Machines (Feature Normalization):

- Kernel Linear - 57%
- Kernel RBF- 47%
- Kernel Poly- 53%

```
-- Anomaly Detection based on One Class Support Vector Machines (PCA Features) --
Obs:  0 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  1 (YouTube ): Kernel Linear->OK         | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  2 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  3 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  4 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  5 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  6 (YouTube ): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  7 (Browsing): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs:  8 (Browsing): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs:  9 (Browsing): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 10 (Browsing): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 11 (Browsing): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 12 (Browsing): Kernel Linear->Anomaly    | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 13 (Browsing): Kernel Linear->Anomaly    | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 14 (P2P     ): Kernel Linear->OK         | Kernel RBF->OK         | Kernel Poly->OK
Obs: 15 (P2P     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 16 (P2P     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 17 (P2P     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 18 (P2P     ): Kernel Linear->OK         | Kernel RBF->OK         | Kernel Poly->OK
Obs: 19 (P2P     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 20 (P2P     ): Kernel Linear->OK         | Kernel RBF->OK         | Kernel Poly->OK
Obs: 21 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->OK         | Kernel Poly->OK
Obs: 22 (VideoCall): Kernel Linear->OK        | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 23 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 24 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->Anomaly    | Kernel Poly->OK
Obs: 25 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->OK         | Kernel Poly->OK
Obs: 26 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 27 (VideoCall): Kernel Linear->Anomaly   | Kernel RBF->OK         | Kernel Poly->Anomaly
Obs: 28 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 29 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 30 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 31 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 32 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 33 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
Obs: 34 (Bot     ): Kernel Linear->OK         | Kernel RBF->Anomaly    | Kernel Poly->Anomaly
```

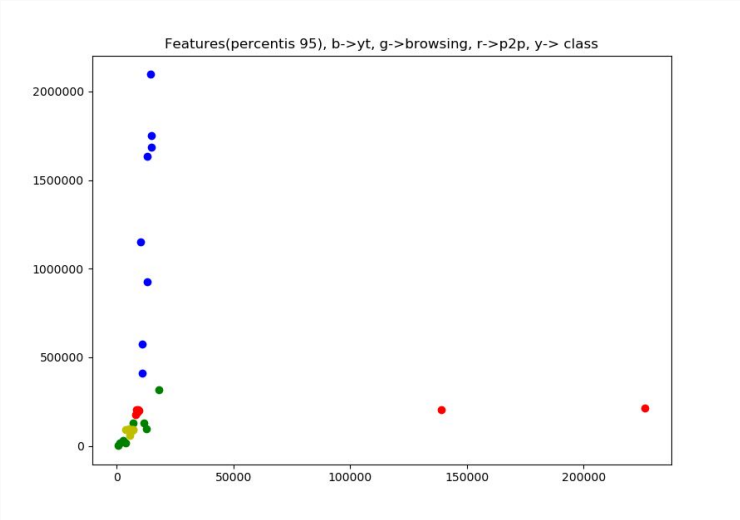
Classificação

Features utilizadas:

- Percentis
- Média e desvio padrão do silêncio (threshold 256 bytes)
- Wavelets

Modelos de Machine Learning:

- Support Vector Machines (permite classificar conjuntos de dados de acordo com os valores das features)
  - com e sem PCA features
  - função linear, rbf e poli kernel
- Neural networks
  - com e sem PCA features



Resultados

Support Vector Machines (Feature Normalization):

- Kernel Linear - 96%
- Kernel RBF- 87%
- Kernel Poly- 92%

Support Vector Machines (PCA Features):

- Kernel Linear - 88%
- Kernel RBF- 83%
- Kernel Poly- 79%

Neural Networks (PCA Features):

- 92%

Neural Networks (Feature Normalization):

- 83%

```
-- Classification based on Support Vector Machines --
Obs:  0 (YouTube ): Kernel Linear->YouTube     | Kernel RBF->Browsing   | Kernel Poly->YouTube
Obs:  1 (YouTube ): Kernel Linear->YouTube     | Kernel RBF->Browsing   | Kernel Poly->YouTube
Obs:  2 (YouTube ): Kernel Linear->YouTube     | Kernel RBF->YouTube    | Kernel Poly->YouTube
Obs:  3 (YouTube ): Kernel Linear->YouTube     | Kernel RBF->YouTube    | Kernel Poly->YouTube
Obs:  4 (YouTube ): Kernel Linear->YouTube     | Kernel RBF->YouTube    | Kernel Poly->YouTube
Obs:  5 (YouTube ): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs:  6 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs:  7 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs:  8 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->YouTube
Obs:  9 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs: 10 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs: 11 (Browsing): Kernel Linear->Browsing    | Kernel RBF->Browsing   | Kernel Poly->Browsing
Obs: 12 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 13 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 14 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 15 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 16 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 17 (P2P     ): Kernel Linear->P2P         | Kernel RBF->P2P        | Kernel Poly->P2P
Obs: 18 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
Obs: 19 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
Obs: 20 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
Obs: 21 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
Obs: 22 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
Obs: 23 (VideoCall): Kernel Linear->VideoCall  | Kernel RBF->VideoCall  | Kernel Poly->VideoCall
```

Obrigado pela vossa atenção