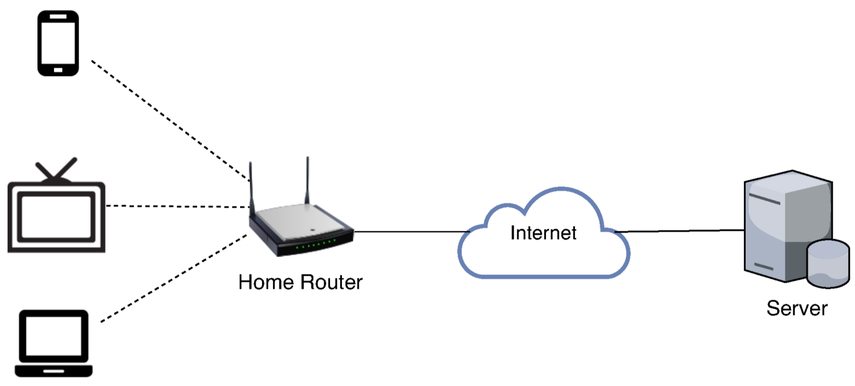
20º WRNP Workshop RNP | 6 E 7 DE MAIO GRAMADO | RS

INSaNE: Improving Network Security at the Network Edge

Coordenadores:
Edmundo de Souza e Silva (UFRJ), Antônio Abelém (UFPA),
Don Towsley (UMass, Amherst)

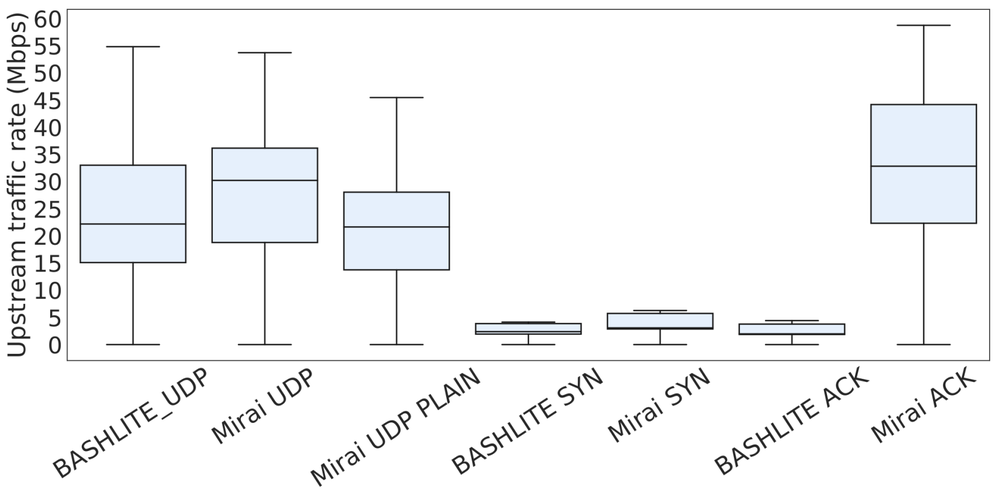
Infraestrutura de medição



- Mais de 4.000 roteadores domésticos
- Latência, perda
- Número de *bytes upstream / downstream*

Uma abordagem leve para detecção de DDoS a partir de roteadores domésticos

- Experimentos



- *Dataset*

Taxa de *upload* dos usuários domésticos
+
Ataques Mirai / BASHLITE

- *Features*

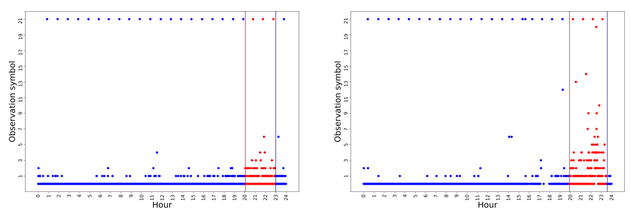
1) Máximo - mínimo	4) Desvio padrão
2) Média	5) Mediana
3) Máximo	6) Mínimo

- Classificador

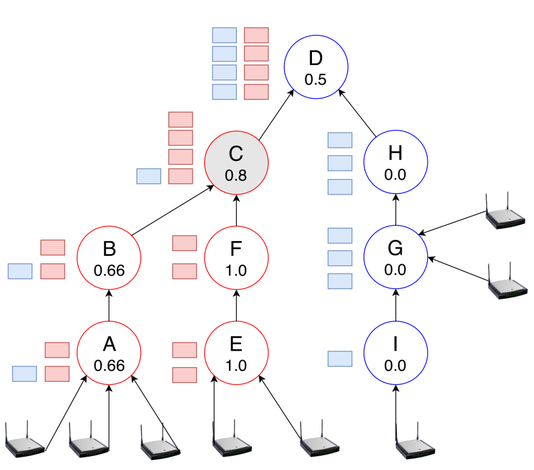
Botnet	Accuracy	Precision	Recall	F1 Score
Mirai	0.999834	0.992327	0.992945	0.992636
BASHLITE	0.999731	0.985987	0.991583	0.988777

Detecção de anomalias a partir de métricas de Qualidade de Serviço

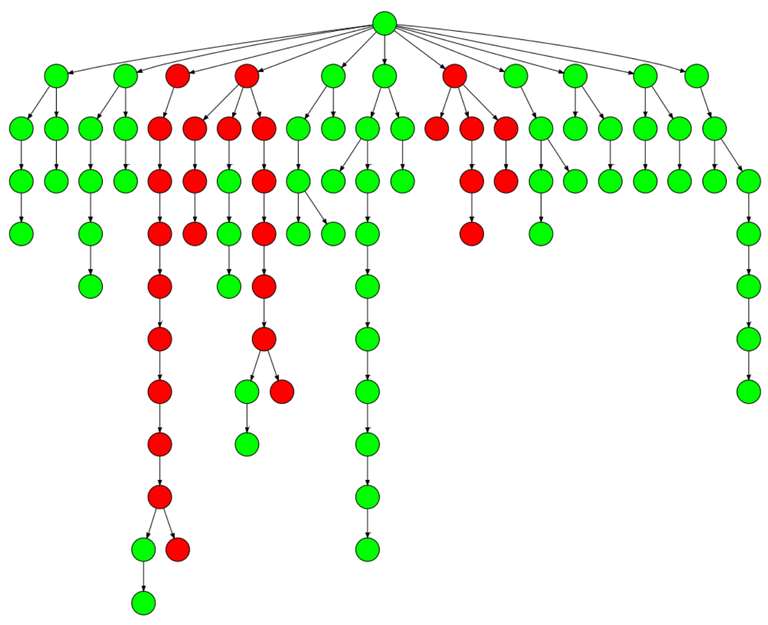
- Modelagem de perda de pacotes



- Votação com base no estado da rede

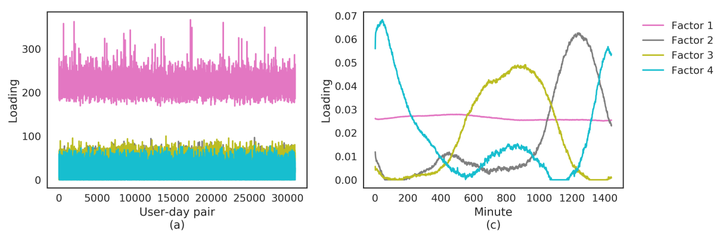


- Detecção de anomalias na rede do provedor

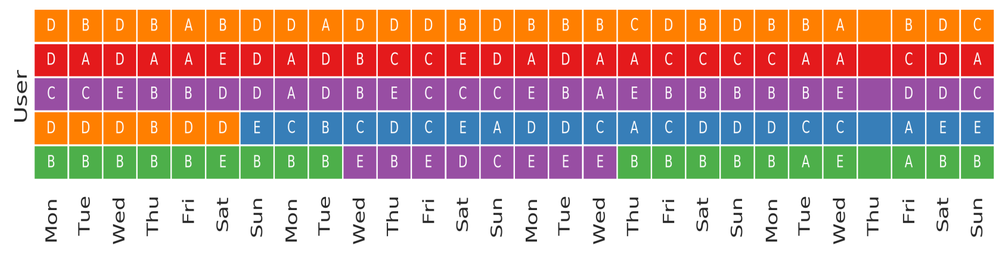


Descobrindo padrões de tráfego de usuários

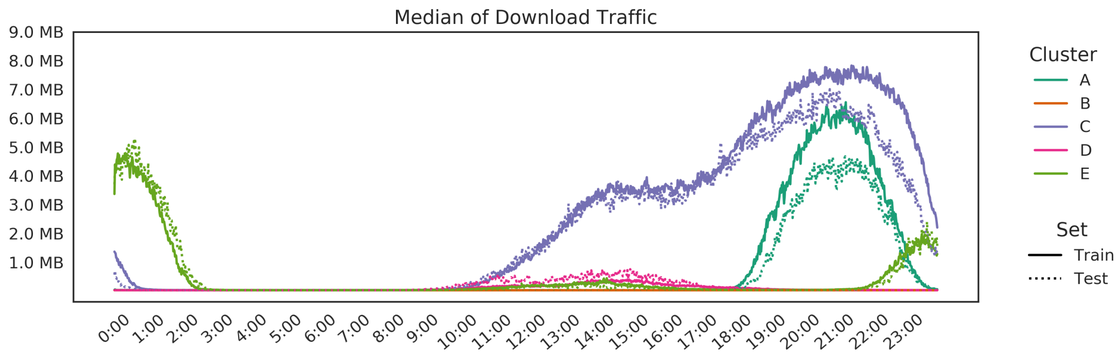
- *Tensor Decomposition*

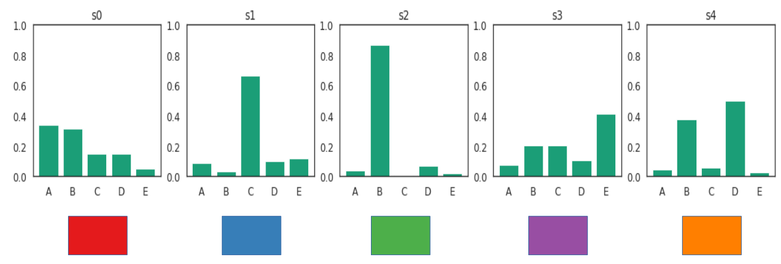


- Comportamento de usuários ao longo dos dias



- Clusterização de pares Usuário-Dia





Experimentos para detecção de DDoS usando dispositivos IoT