

Plano de Execução

Para comparação os seguintes algoritmos serão aplicados (divididos em categorias):

- Clustering:
 - Kmeans: largamente conhecido na literatura, é capaz de processar uma grande quantidade de amostras e um número médio de clusters. É usado para casos gerais, por isso é relevante no estudo. Vale ressaltar que não é desejável sua aplicação para uma quantidade elevada de clusters. Parâmetro: número de clusters.
 - Ward hierarquical clustering: capaz de processar grandes amostras e vários clusters. Se adequa ao cenário do trabalho. Parâmetro: número de clusters.
 - DBSCAN: capaz de processar amostras muito grandes e um número elevado de clusters. Parâmetro: tamanho da vizinhança.
 - Outlier detection: http://scikit-learn.org/stable/modules/outlier_detection.html. Scikit-learn fornece
 - HBOS: escolhido devido ao desempenho apresentado em outros trabalhos.
- Para os ataques do tipo DoS (Denial of Service) as features escolhidas são: “source bytes” e “percentage of packets with errors”. Escolha baseada em outros trabalhos.