Análise do desempenho de Honeypots e algoritmos de Machine Learning em tarefas de detecção de intrusão

unesp

Orientador: Kelton Augusto Pontara Costa
Orientando: Renato Leite Camilo

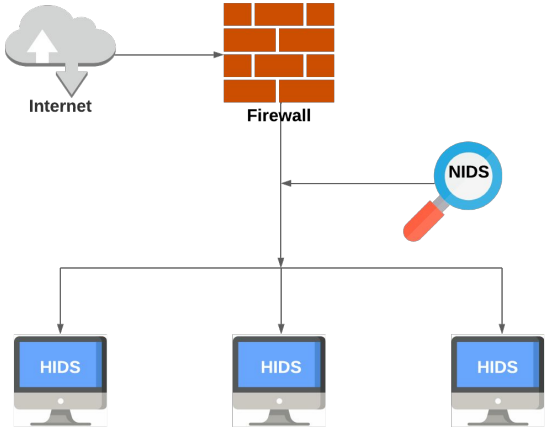
Introdução

Um problema constante

1. **Crescimento** no número de ataques cibernéticos
2. Foram registradas no Brasil **32 bilhões** de tentativas de ataques cibernéticos no primeiro semestre de 2022

Mecanismos que podem ser melhorados

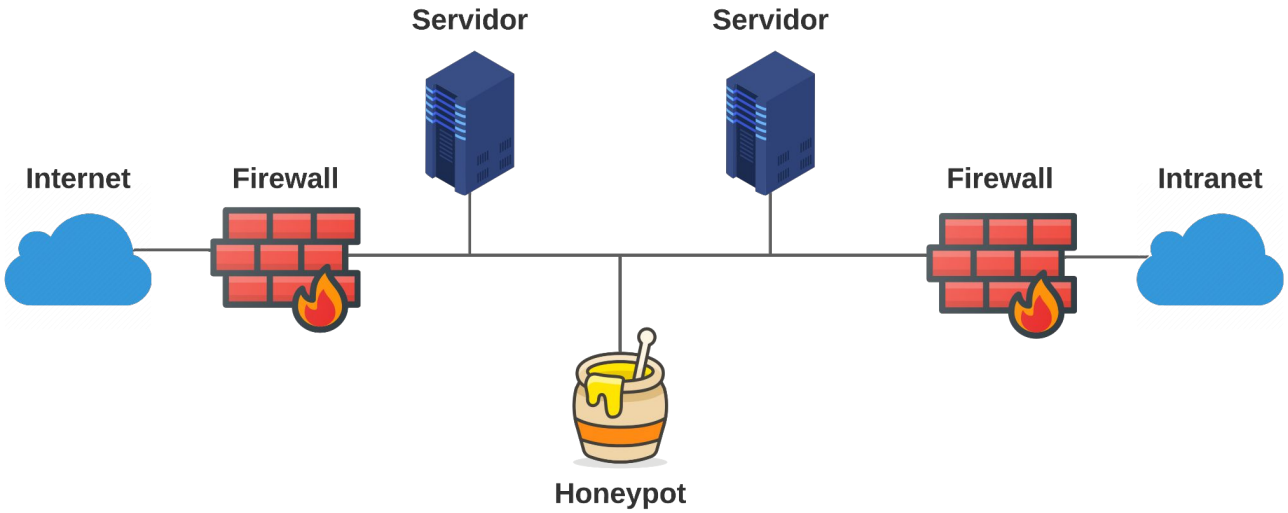
1. Sistemas de detecção de intrusão possuem **deficiências**
2. Alta taxa de **falsos positivos**
3. Soluções que empregam ***machine learning***



Fundamentação teórica

Honeypot

- É definido como uma **armadilha** para invasores
- Toda interação com um *honeypot* **é um ataque**



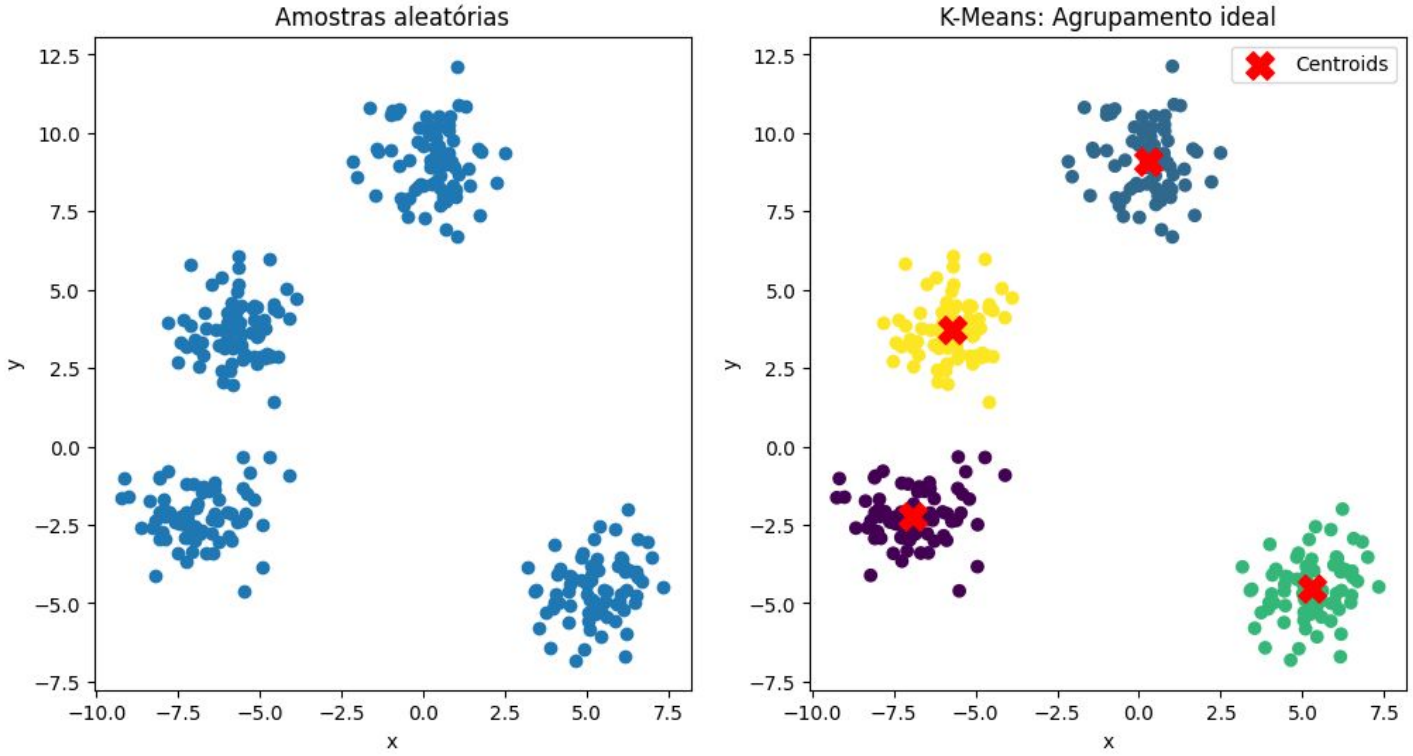
Algoritmos supervisionados

- Foram selecionados **três** algoritmos supervisionados para estudo
  - Support Vector Machine
  - Multilayer Perceptron
  - K-Nearest Neighbors
- Critério de escolha foi o **desempenho** em outros trabalhos

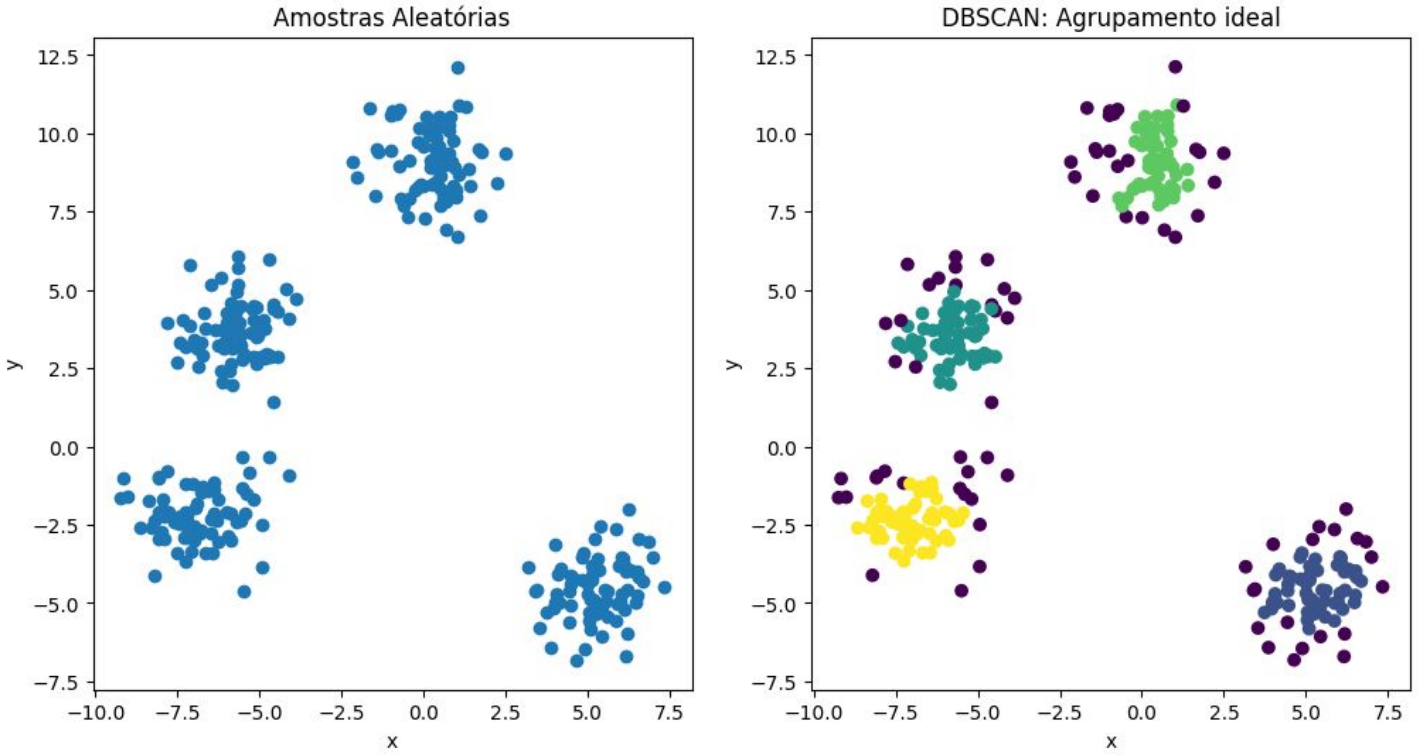
Algoritmos não supervisionados

- Foram selecionados **dois** algoritmos não supervisionados para estudo
  - K-Means: baseado em centróides
  - DBSCAN: baseado em densidade
- K-Means é um dos **mais conhecidos** em *machine learning*
- DBSCAN é um algoritmo que lida bem com **dados discrepantes**

K-Means: um exemplo de clustering



DBSCAN: um exemplo de clustering



Metodologia

Kyoto Dataset +2006

- Conjunto de dados preparado com o auxílio de ***honeypots***
- Originado de **tráfego real**
- **24 atributos** para análise

Atributo	Tipo
Duration	float64
Service	object
Source bytes	int64
Destination bytes	int64
Count	int64
Same srv rate	float64
Serror rate	float64
Srv serror rate	float64
Dst host count	int64
Dst host srv count	int64
Dst host same src port rate	float64
Dst host serror rate	float64
Dst host srv serror rate	float64
Flag	object
IDS detection	object
Malware detection	object
Ashula detection	object
Label	int64
Source IP Address	object
Source Port Number	int64
Destination IP Address	object
Destination Port Number	int64
Start Time	object
Protocol	object

KDD Cup 1999

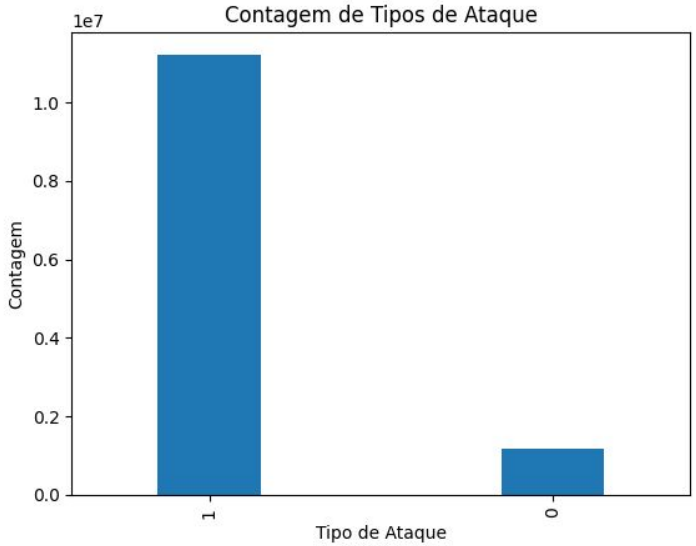
- Conjunto de dados elaborado para uma **competição de detecção de intrusão**
- Originado de **tráfego simulado**
- **41 atributos** para análise

Atributo	Tipo
duration	int64
Protocol	int64
Service	int64
flag	object
src_bytes	int64
Destination bytes	int64
land	int64
wrong_fragment	int64
urgent	int64
hot	int64
num_failed_logins	int64
logged_in	int64
num_compromised	int64
root_shell	int64
su_attempted	int64
num_root	int64
num_file_creations	int64
num_shells	int64
num_access_files	int64
num_outbound_cmds	int64
is_host_login	int64

Atributo	Tipo
is_guest_login	int64
Count	int64
srv_count	int64
serror_rate	float64
srv_serror_rate	float64
rerror_rate	float64
srv_rerror_rate	float64
same_srv_rate	float64
diff_srv_rate	float64
srv_diff_host_rate	float64
Dst host count	int64
dst_host_srv_count	int64
dst_host_same_srv_rate	float64
dst_host_diff_srv_rate	float64
dst_host_same_src_port_rate	float64
dst_host_srv_diff_host_rate	float64
dst_host_serror_rate	float64
dst_host_srv_serror_rate	float64
dst_host_rerror_rate	float64
dst_host_srv_rerror_rate	float64
Label	int64

Situação do conjunto de dados

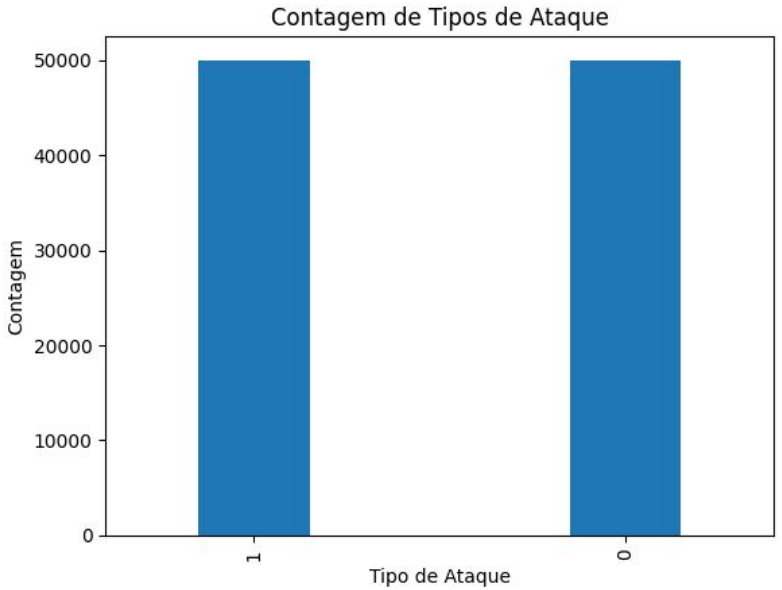
- Dados de **diferentes tipos**
- Dados **desbalanceados**



Atributo	Tipo
Duration	float64
Service	object
Source bytes	int64
Destination bytes	int64
Count	int64
Same srv rate	float64
Serror rate	float64
Srv serror rate	float64
Dst host count	int64
Dst host srv count	int64
Dst host same src port rate	float64
Dst host serror rate	float64
Dst host srv serror rate	float64
Flag	object
IDS detection	object
Malware detection	object
Ashula detection	object
Label	int64
Source IP Address	object
Source Port Number	int64
Destination IP Address	object
Destination Port Number	int64
Start Time	object
Protocol	object

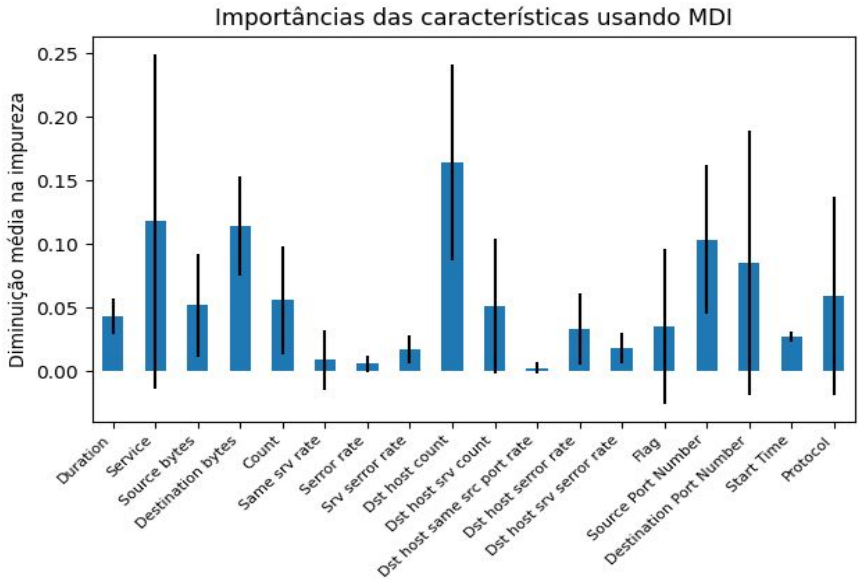
Pré-processamento

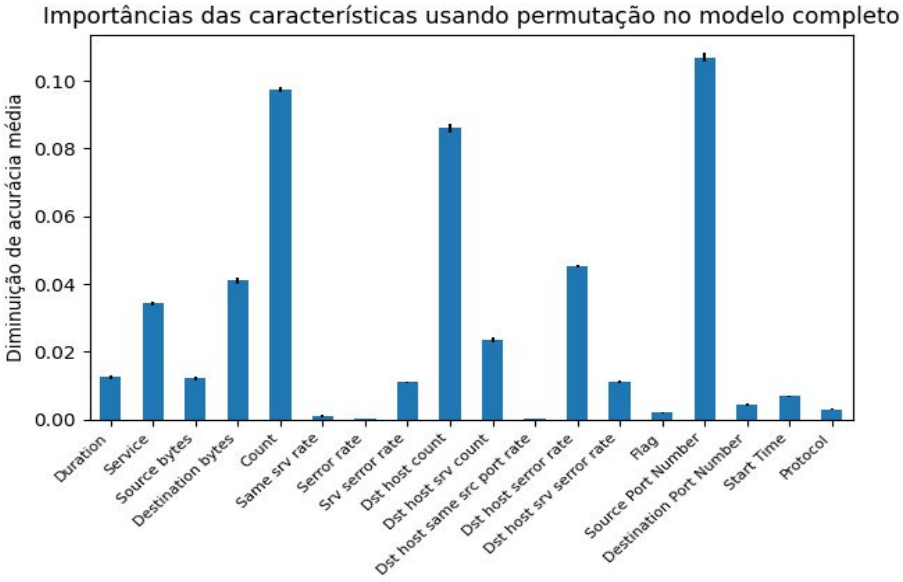
- **Unificação** dos tipos de dados
- **Balanceamento** das amostras
  - Downsampling
- **Normalização** dos dados
  - Normalizer



Seleção de características

- Emprego do algoritmo ***Random Forest***
- **Extração de características** usando *feature importance*

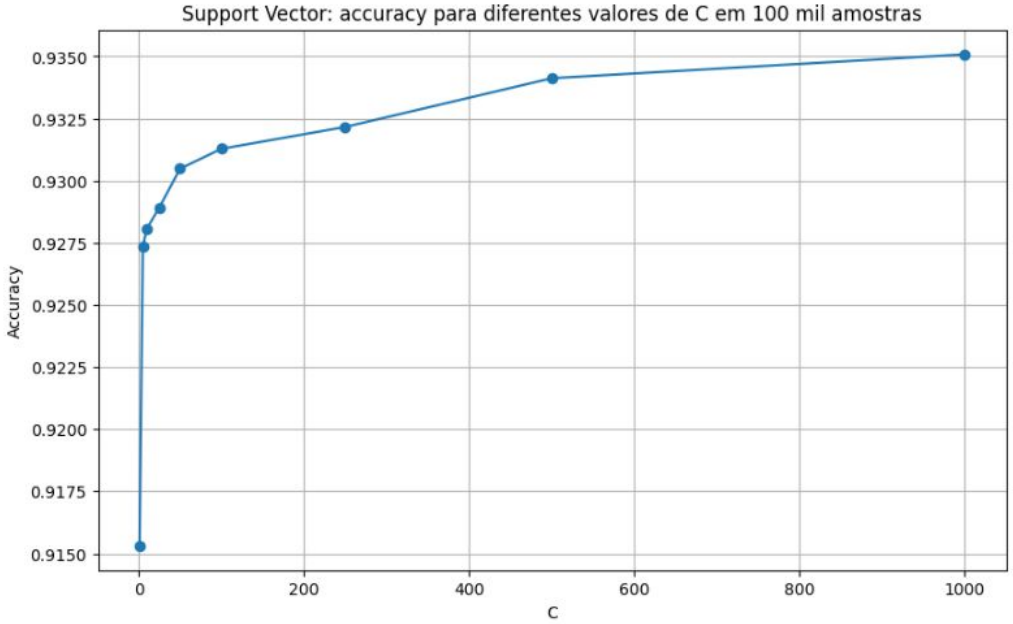




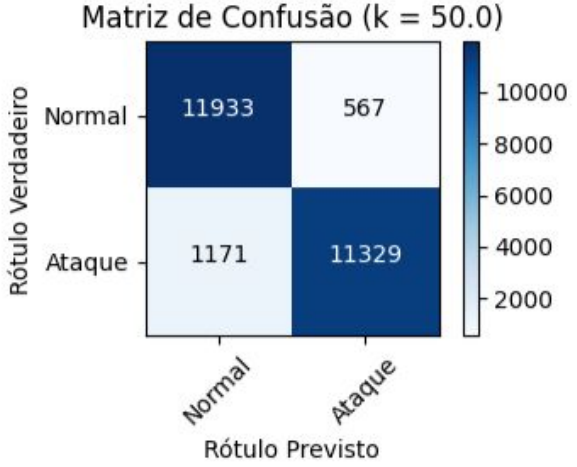
Treinamento dos modelos

- Etapa para **ajustar** os parâmetros dos modelos
- Treinamento com **100 mil** amostras
- SVM **(parâmetro C)**
- MLP **(ativador e otimizador)**
- KNN **(número de vizinhos)**

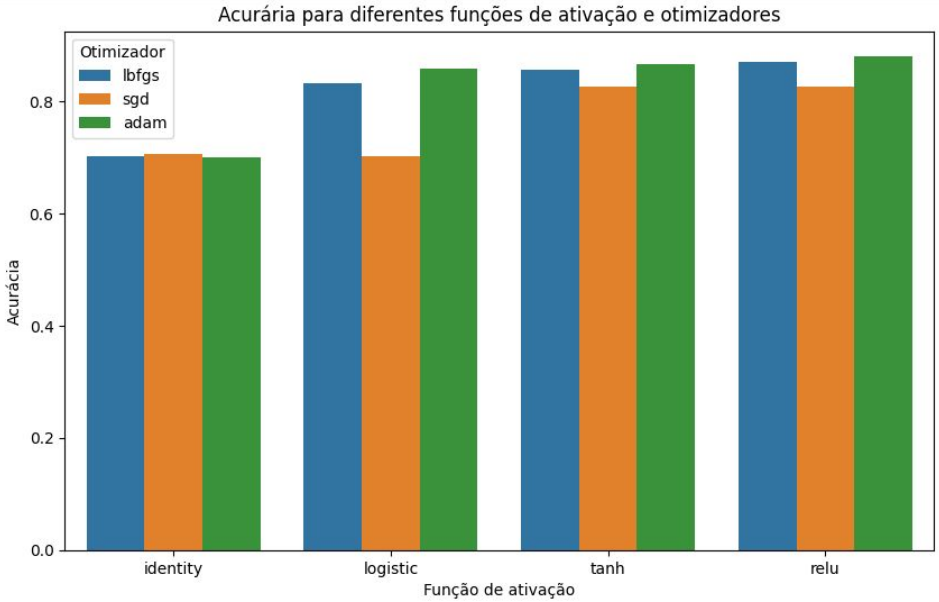
SVM



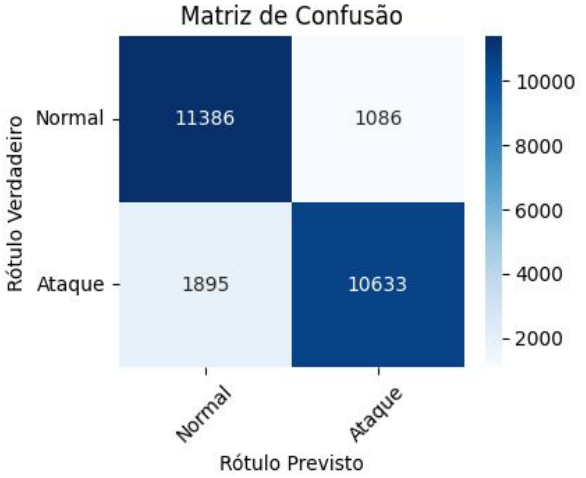
C	Acurácia	Precisão	Recall	F1-Score
n = 1	92%	95%	88%	91%
n = 5	93%	95%	90%	93%
n = 10	93%	95%	90%	93%
n = 25	93%	95%	90%	93%
n = 50	93%	95%	91%	93%
n = 100	93%	95%	91%	93%
n = 250	93%	95%	91%	93%
n = 500	93%	95%	91%	93%
n = 1000	94%	95%	91%	93%



MLP

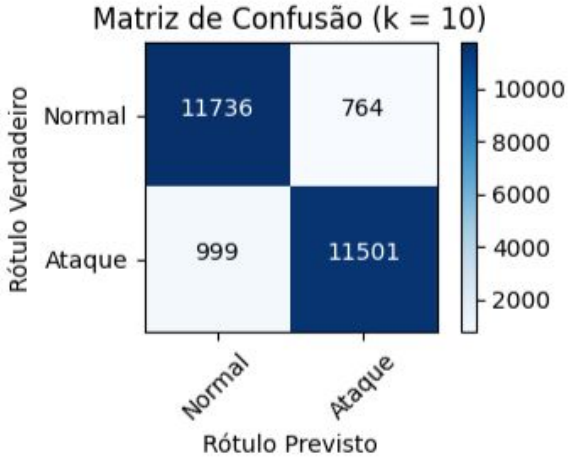


Ativação	Otimizador	Acurácia	Precisão	Recall	F1-Score
identity	lbfgs	68%	73%	59%	65%
identity	sgd	68%	72%	61%	66%
identity	adam	68%	73%	59%	65%
logistic	lbfgs	83%	86%	79%	82%
logistic	sgd	68%	72%	61%	66%
logistic	adam	82%	87%	76%	81%
tanh	lbfgs	86%	88%	84%	86%
tanh	sgd	69%	73%	61%	66%
tanh	adam	85%	89%	81%	85%
relu	lbfgs	88%	88%	87%	88%
relu	sgd	80%	85%	73%	78%
relu	adam	86%	90%	82%	86%



KNN

Vizinhos	Acurácia	Precisão	Recall	F1-Score
n = 5	93%	93%	92%	93%
n = 10	93%	94%	92%	93%
n = 25	93%	94%	91%	93%
n = 50	92%	94%	90%	92%
n = 100	92%	94%	89%	92%
n = 250	91%	94%	88%	90%
n = 500	90%	94%	87%	90%
n = 1000	90%	94%	86%	89%



Análises e resultados

Eficácia geral

Kyoto Dataset +2006

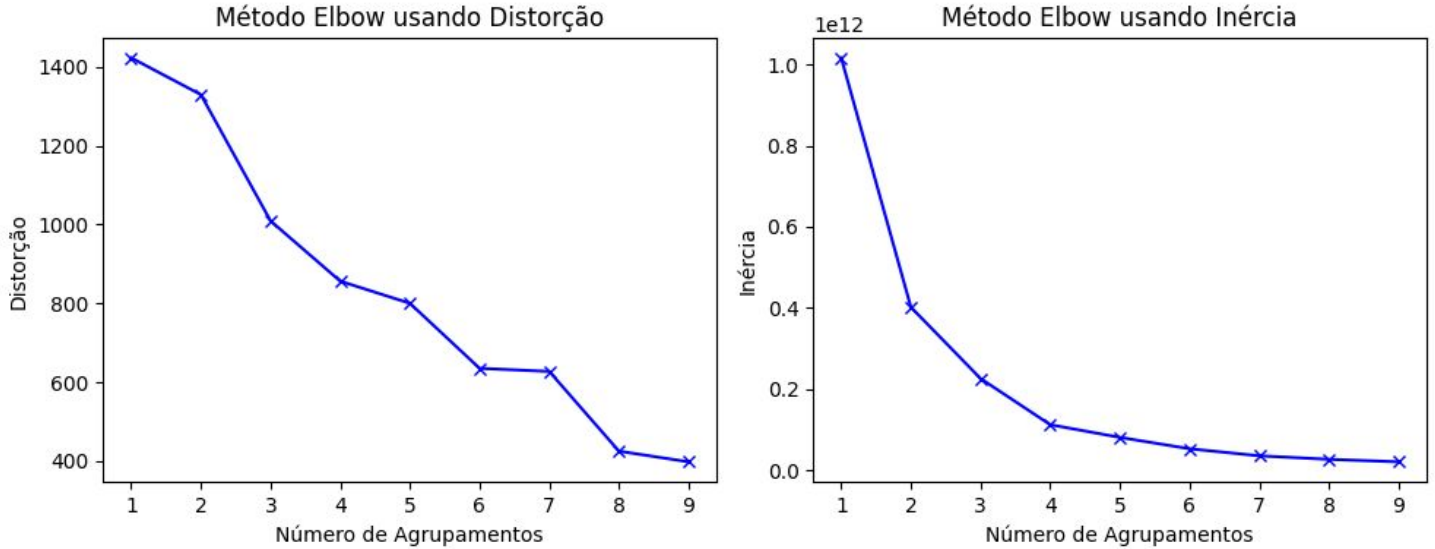
Algoritmo	Acurácia	Precisão	Recall	F1-Score
SVM	86%	90%	81%	85%
MLP	88%	86%	91%	88%
KNN	90%	89%	92%	90%

KDD Cup 1999

Algoritmo	Acurácia	Precisão	Recall	F1-Score
SVM	80%	76%	88%	82%
MLP	75%	67%	99%	80%
KNN	72%	68%	82%	74%

Observação para clustering

- **Método Elbow** para determinar número de centróides para o algoritmo K-Means



Após clustering

Kyoto Dataset +2006

Algoritmo	Acurácia	Precisão	Recall	F1-Score	Técnica
SVM	90% (+4%)	90%	91% (+10%)	90% (+5%)	DBSCAN 10
MLP	89% (+1%)	92% (+6%)	85% (-6%)	88%	DBSCAN 10
KNN	91% (+1%)	90% (+1%)	93% (+1%)	91% (+1%)	DBSCAN 10

KDD Cup 1999

Algoritmo	Acurácia	Precisão	Recall	F1-Score	Técnica
SVM	80%	76%	88%	82%	-
MLP	79% (+4%)	70% (+3%)	99%	82% (+2%)	DBSCAN 100
KNN	72%	68%	84%	75%	-

Considerações finais

Considerações finais

- Implementar uma rede real com **honeypots**
- Experimentar outros **algoritmos** e **técnicas**
- Analisar **outras abordagens** de algoritmos de clustering

unesp

Obrigado!