Avaliando algoritmos de classificação em Fluxos de dados aplicados na detecção de ataques à rede usando o MOA (Massive Online Analysis)

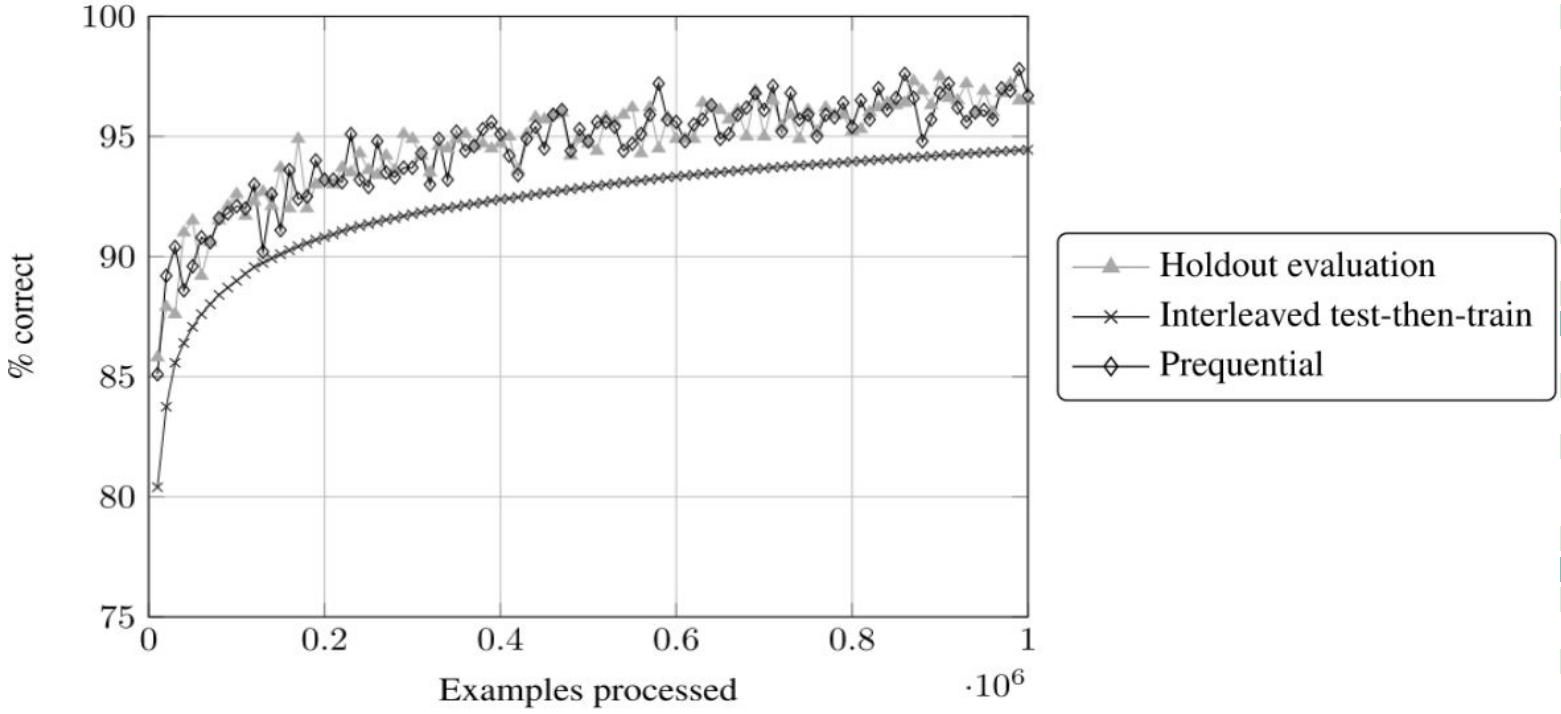
Alunos:
Augusto Parisot de Gusmão Neto
Marcelo Marques da Rocha

ROTEIRO

1. Introdução
2. Metodologia da Análise Experimental
3. Resultados Obtidos
4. Conclusão

Metodologia da Análise Experimental

(Avaliação de Classificadores em Fluxo de Dados)



Metodologia da Análise Experimental
(Classificadores utilizados)

- Majority Class
- No-Change
- Naive Bayes
- Perceptron
- KNN
- Hoeffding Tree
- Hoeffding Option Tree
- Hoeffding Adaptive Tree

Metodologia da Análise Experimental
(Dataset Utilizado)

- Copa KDD 1999
- 39 tipos de ataque
- Desempenho dos classificadores depende do dataset
- LGPD
- Problema do Oráculo
- NSL-KDD

Metodologia da Análise Experimental

(Dataset Utilizado - Tipos de ataque)

Tabela 1. Tipos de ataques e suas respectivas quantidades de ocorrências no Dataset

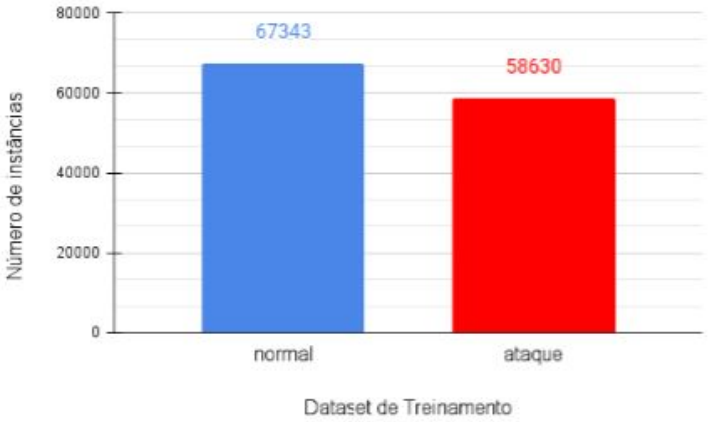
#	Ataque	Qtd.	#	Ataque	Qtd.	#	Ataque	Qtd.	#	Ataque	Qtd.
1	neptune	45871	11	teardrop	904	21	buffer_overflow	50	31	loadmodule	11
2	satan	4368	12	warezclient	890	22	multihop	25	32	xlock	9
3	ipsweep	3740	13	apache2	737	23	land	25	33	phf	6
4	smurf	3311	14	processtable	685	24	rootkit	23	34	perl	5
5	portsweep	3088	15	snmpguess	331	25	named	17	35	xsnoop	4
6	nmap	1566	16	saint	319	26	ps	15	36	spy	2
7	back	1315	17	mailbomb	293	27	sendmail	14	37	worm	2
8	guess_passwd	1284	18	pod	242	28	xterm	13	38	sqlattack	2
9	msca	996	19	snmpgetattack	178	29	imap	12	39	udpstorm	2
10	warezmaster	964	20	httptunnel	133	30	ftp_write	11			

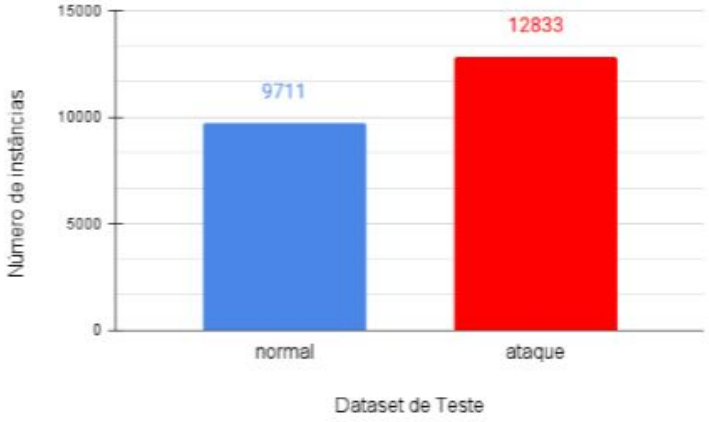
Metodologia da Análise Experimental
(Dataset Utilizado)

- Copa KDD 1999
- 39 tipos de ataque
- Desempenho dos classificadores depende do dataset
- LGPD
- Problema do Oráculo
- NSL-KDD

Metodologia da Análise Experimental

(Dataset Utilizado – Divisão de Classes do Experimento)





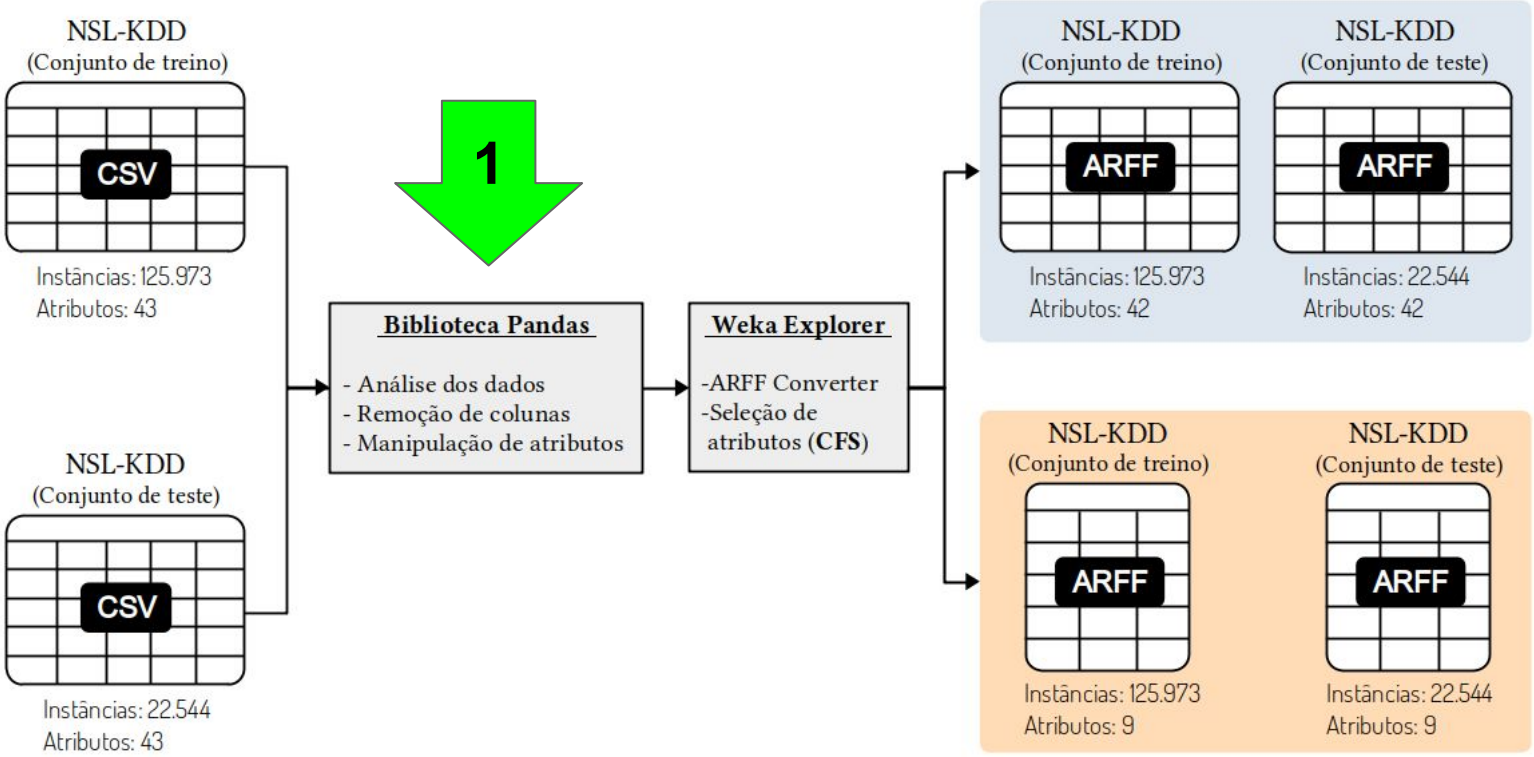
Metodologia da Análise Experimental

(Ambiente de Experimentação e Análise)

Massive Online Analysis

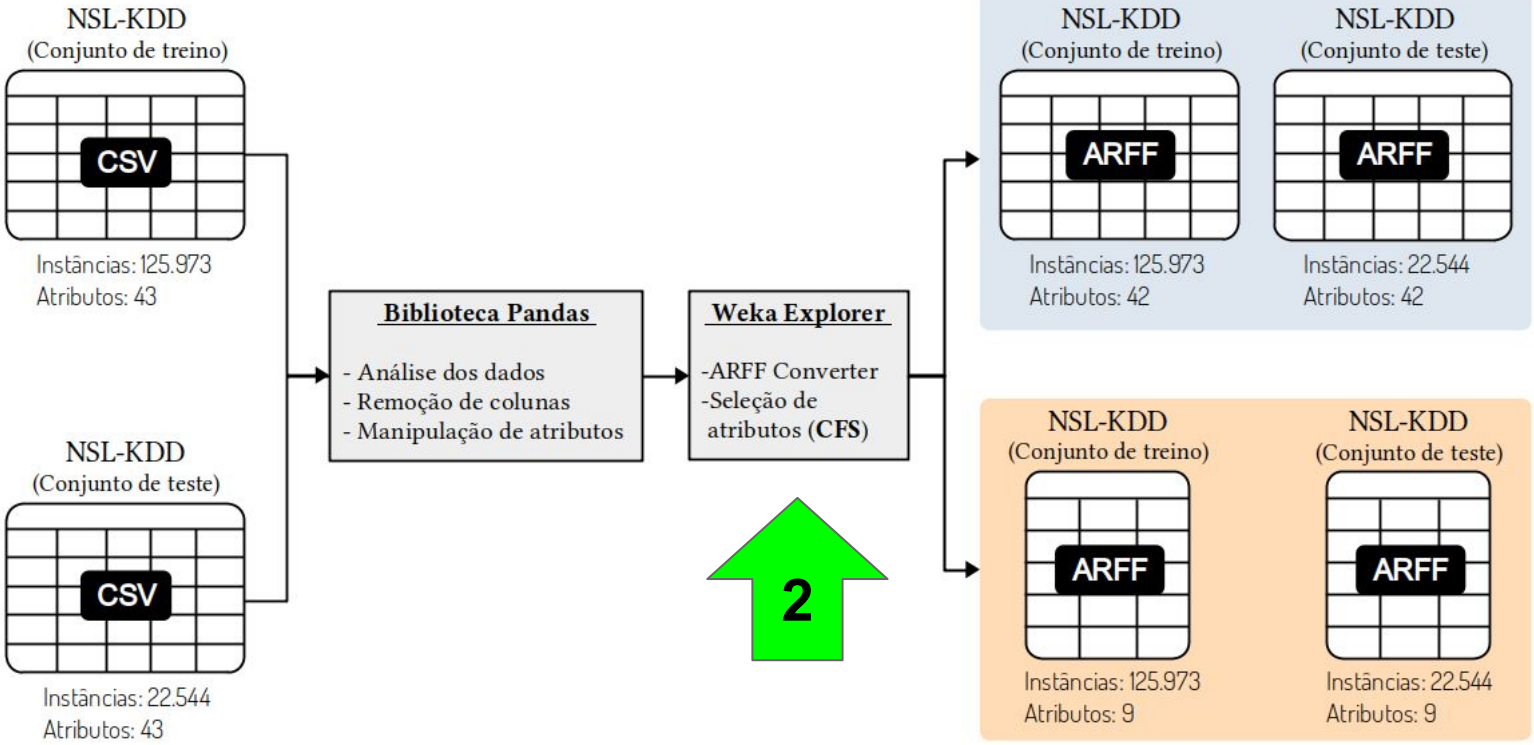
Metodologia da Análise Experimental

(0 Experimento - Processamento do Dataset)



Metodologia da Análise Experimental

(0 Experimento – Processamento do Dataset)

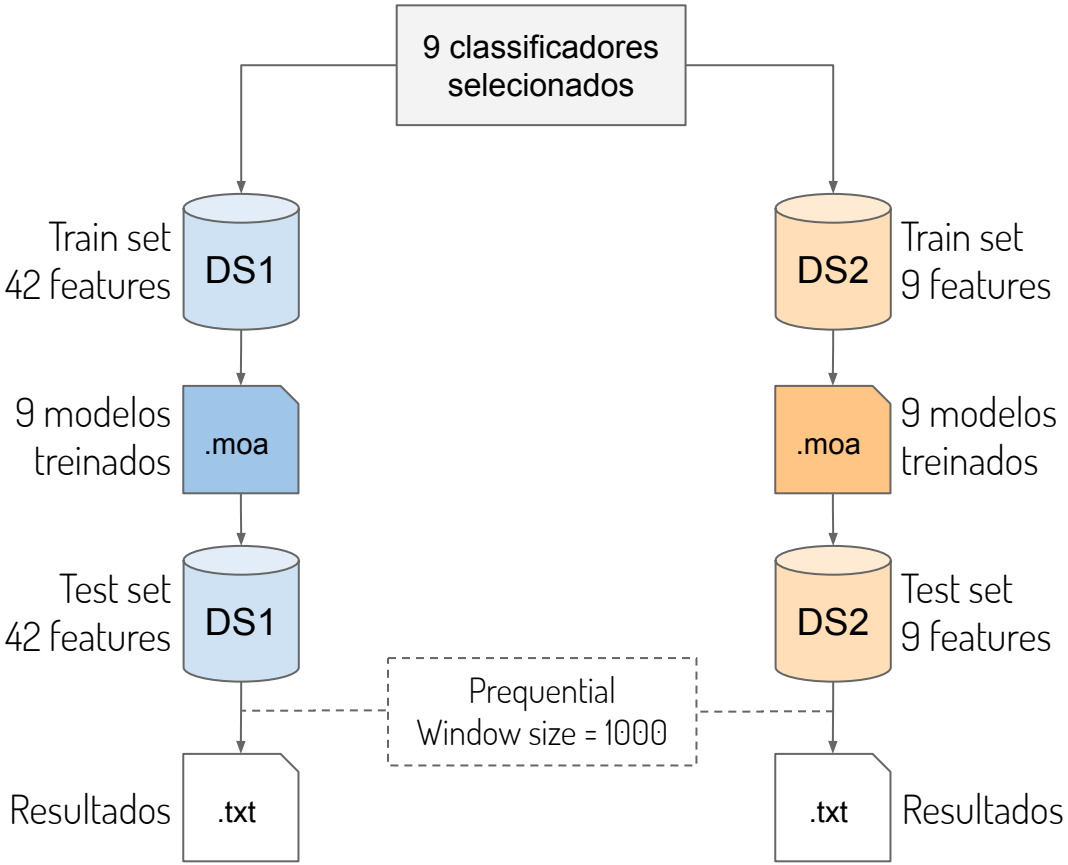


Metodologia da Análise Experimental
(O Experimento)

- Avaliar os classificadores sobre o dataset 1 (DS1) com 42 features
- Avaliar os classificadores sobre o dataset 2 (DS2) com 9 features

Metodologia da Análise Experimental

(0 Experimento - Treinamento e Teste)



Metodologia da Análise Experimental

(O Experimento – Resultados das avaliações)

Tabela 2. Avaliação dos modelos treinados nos dois Datasets - Prequential(window size = 1000)

Classificador (Modelo treinado)	Dataset 1 (42 atributos)					Dataset 2 (9 atributos)				
	Acurácia (%)		Tempo	Precisão (%)		Acurácia (%)		Tempo	Precisão (%)	
	MD	D.P	[CPU]	Normal	Ataque	MD	D.P	[CPU]	Normal	Ataque
Majority Class	43,03	1,79	0,11	43,03	0,00	43,03	1,79	0,04	43,03	0,00
No-change	50,60	1,93	0,16	42,54	56,58	50,60	1,93	0,03	42,54	56,58
Naive Bayes	78,88	1,80	0,14	69,10	92,11	73,67	1,50	0,12	62,40	96,91
Decision Stump	81,63	2,48	2,62	73,94	89,95	69,92	1,51	0,95	59,08	96,74
Hoeffding Tree	94,05	0,92	0,68	91,15	96,42	90,09	1,82	0,14	84,17	95,79
Hoeffding Adaptive Tree	94,97	1,33	0,79	91,88	97,59	82,38	1,81	0,34	83,68	83,92
Hoeffding Option Trees	94,09	0,90	0,93	91,22	96,43	89,72	3,48	0,64	84,75	94,70
Perceptron	43,03	1,79	0,16	43,03	4,35	71,20	1,74	0,06	59,99	98,85
KNN	95,07	1,31	5,99	95,01	95,19	92,33	1,45	1,66	92,60	92,16

Metodologia da Análise Experimental

(O Experimento - Ranking de Classificadores)

- A comparação foi feita entre mais de dois modelos
- A comparação foi feita por pares
- Foi utilizado o teste de *Friedman* e o pós-teste de *Nemenyi*

Metodologia da Análise Experimental

(0 Experimento - Ranking de Classificadores)

- Tipo de pós-teste: *Nemenyi*
- p-Value: 0.05 (default)
- Métrica: Percentual de classificações corretas
- Tipo: Média

Resultados Obtidos

(Ranking dos Classificadores)

Tabela 3. Ranqueamento dos classificadores nos dois Datasets - Métrica (Percentual médio de acertos)

Ranking	Dataset 1 (42 atributos)				Dataset 2 (9 atributos)			
	Classificador (Modelo treinado)	Acurácia (%) MD	D.P	Tempo [CPU]	Classificador (Modelo treinado)	Acurácia (%) MD	D.P	Tempo [CPU]
1º	KNN	95,07	1,31	5,99	KNN	92,33	1,45	1,66
2º	Hoeffding Adaptive Tree	94,97	1,33	0,79	Hoeffding Tree	90,09	1,82	0,14
3º	Hoeffding Option Tree	94,09	0,90	0,93	Hoeffding Option Tree	89,72	3,48	0,64
4º	Hoeffding Tree	94,05	0,92	0,68	Hoeffding Adaptive Tree	82,38	1,81	0,34
5º	Decision Stump	81,63	2,48	2,62	Naive Bayes	73,67	1,50	0,12
6º	Naive Bayes	78,88	1,80	0,14	**Perceptron**	**71,20**	**1,74**	**0,06**
7º	No-change	50,60	1,93	0,16	Decision Stump	69,92	1,51	0,95
8º	Perceptron	43,03	1,79	0,16	No-change	50,60	1,93	0,03
9º	Majority Class	43,03	1,79	0,11	Majority Class	43,03	1,79	0,04

Conclusão

- Avaliação da acurácia
- Trabalhando com dataset em 2 versões
- Pandas Weka Explorer
- MOA
- Desempenho dos classificadores (acurácia e tempo de CPU)
- Friedman
- Nemenyi

Obrigado.