Deteção de Drones Intrusos

Luiz C. Giacomossi Jr. [1], **Livia Fragoso Pimentel** [1], **Jefferson Costa de Matos** [1]

[1]Instituto de Tecnológico de Aeronáutica (ITA)
São José dos Campos – SP – Brasil

luiz.giacomossi@ga.ita.br, livia.pimentel@ga.ita.br, jefferson.matos@ga.ita.br

[2]PO-233 - Aprendizado de Máquina
Entrega do Projeto Final

Resumo. *A crescente aplicação de drones possibilitou o advento de novas soluções para os desafios do mundo moderno e expôs a necessidade de maior atenção a questões relacionadas a segurança e privacidade. Nesse contexto, a identificação de drones invasores representa uma solução urgente em meio ao aumento dos riscos decorrentes da popularização desse tipo de veículo. Frente a esse cenário, este estudo visa a aplicar técnicas de Aprendizado de Máquina na detecção de drones invasores com o uso de dados de tráfego wi-fi criptografados. A metodologia aplicada baseia-se em uma análise exploratória desses dados, seguida da etapa de pré-processamento e a indução de um modelo de Aprendizagem de Máquina, para classificar se o sinal é de um drone, ou não.*

1. Introdução

Os veículos aéreos não tripulados (VANTs), comumente chamados de drones, são empregados em diversas aplicações como lazer, captura de imagens, operações logísticas de proximidade com o cliente (como *last mile delivery*), inspeções técnicas em locais de difícil acesso e monitoramento. Este mercado tem crescido significativamente nos últimos anos e há uma corrida global entre os países desenvolvidos pela vanguarda do desenvolvimento deste tipo de veículo [Schroth 2020] [Boyle 2015].

Apesar da sua ampla aplicabilidade, o uso de drones ainda enfrenta diversos desafios relacionados ao controle do espaço aéreo e a questões ligadas à proteção de privacidade. No Brasil, como a regulamentação do uso desses veículos ainda é incipiente, algumas restrições práticas apresentam-se como, por exemplo, a impossibilidade de utilizá-los largamente em regiões próximas a centros urbanos.

Como destacado, o aumento de VANTs possibilita riscos potenciais para a segurança pública e a privacidade pessoal. Para minimizar estes riscos, detectar e identificar com eficiência os VANTs invasores é uma necessidade urgente. Os métodos de detecção física existentes (como radar, visão e som) podem ser ineficazes em alguns cenários. Para contornar esses problemas, os registros de dados de tráfego wi-fi dos VANTs são uma fonte promissora de detecção de drones invasores.

Diante desse cenário, pretende-se aplicar técnicas de aprendizagem de máquina para detecção de drones intrusos, explorando os dados existentes provenientes de sinais de wi-fi criptografados de VANTs comerciais. Em uma análise prévia, constata-se que é possível aplicar técnicas de aprendizagem supervisionada, uma vez que o problema em questão trata-se de uma tarefa preditiva de classificação binária. Ademais, além da precisão dessa classificação, o tempo de execução de previsão do método do detector também

é importante, visto que os intrusos voam a uma velocidade considerável. Portanto, será necessário otimizar em conjunto o tempo de execução da previsão e sua precisão.

Este artigo é constituído de um breve referencial teórico sobre o tema (Seção 2), seguido da Seção 3, onde serão descritos os métodos e as técnicas usados no tratamento e na caracterização dos dados. A seção 4 é dedicada aos experimentos aos quais a base foi submetida, para a posterior aplicação de um modelo de Aprendizado de Máquina. Por fim, na parte 5 encontram-se discussões dos resultados apresentados e em seguida a conclusão será apresentada.

2. Bibliografia Correlata

Há trabalhos que focam nos desafios enfrentados no controle de drones visando a manutenção da privacidade e da inviolabilidade da propriedade privada, bem como aspectos éticos de seu uso [Altawy and Youssef 2016]. Além disso, há projetos concentrados na segurança cibernética, mostrando experiências e referências que evidenciam as vulnerabilidades e ameaças em possíveis ataques a sistemas de drones [Ulrich and Nobre 2019].

No caso de identificação de drones, a criação de um ambiente chamado Internet de Drones (IoD) também é um tema recorrente [Gharibi and Waslander 2016]. Nesse contexto, os dados seriam transmitidos entre o drone e a estação terrestre de controle, sendo que os dados suspeitos, isto é, potencialmente não autorizados, seriam armazenados em uma *blockchain* privada.

Especificamente em relação a drones intrusos, a integração de drones em cidades inteligentes, os mecanismos de bloqueios de VANTs em áreas perigosas e não autorizadas também representam temas oportunos [Vattapparamban and Uluagaç 2016]. Nesse contexto, contudo, o foco é no sistema de interrupção do drones, com uso de diversas técnicas que passam por aves treinadas para capturas até o impedimentos por outros drones, não focando, contudo, no problema de detecção.

Um exemplo de uso de Aprendizado de Máquina para identificar tipos de drones apenas com parâmetros básicos dos sinais wi-fi transmitidos por VANTs, tais como tamanho da mensagem, espaço de tempo entre elas e outros parâmetros estatísticos são demonstrados em [Alipour-Fanid and Zhao 2020] .

3. Materiais e Métodos

Neste projeto, a manipulação dos dados e a geração de um modelo preditivo de aprendizado serão implementados por meio da biblioteca Scikit-learn, da linguagem Python. A seguir, serão detalhados os métodos e as ferramentas utilizados nesse estudo com o objetivo de construir tal modelo para a detecção de drones intrusos.

3.1. Conjunto de Dados

Para a detecção VANTs intrusos será utilizado o conjunto de dados disponibilizado em [Zhao 2018]. Estes dados são provenientes de um sistema de detecção de sinais wi-fi e captura de pacotes que pode coletar todo o tráfego wi-fi dentro de uma faixa de detecção física em tempo real. Podem haver vários usuários de Wi-Fi na faixa de detecção, sendo estes VANTs ou dispositivos não-VANTs, como computadores e celulares.

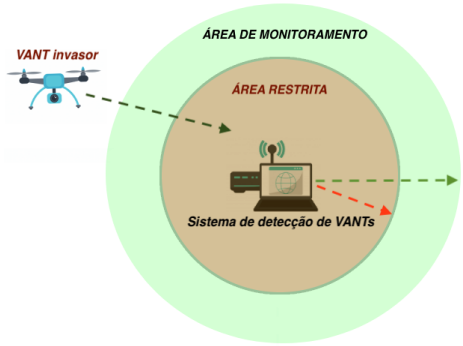

Figura 1. Sistema de captura dos dados

Este sistema de detecção, descrito na figura 1, captura pacotes de dados (criptografados e não-criptografados) dentro de uma área delimitada, com o uso do software wireShark [Wireshark]. Para dados sem criptografia, assume-se que o sistema pode descobrir o tipo de aplicativo de origem examinando o conteúdo do pacote. Logo, este estudo irá se concentrar apenas no tráfego Wi-Fi criptografado.

Para este problema, a abordagem para o desenvolvimento da base de dados foi baseada na criação de uma representação compacta dos dados brutos de fluxo de rede no intervalo de tempo. Esta representação contém um conjunto de características estatísticas calculados a partir dos dados brutos de rede. Seguindo esta ideia, seis conjuntos de dados reais para detecção de intrusos estão disponibilizados. Especificamente, os dados de rede contendo fluxos de drones intrusos e não-drones. Para a obtenção dos dados de VANTs, foram capturados dados a partir de três modelos de drones comerciais, vistos na figura 2.

(a) Parrot Bebop 1 (b) DBPower UDI (c) DJI Spark

Figura 2. Drones comerciais utilizados [Zhao 2018].

Assim, estes conjuntos de dados são combinações entre os diferentes tipos de VANTs e modos de tráfego, conforme a tabela 3.1.

Tabela 1. Conjuntos de dados dos drones comerciais em dois modos de tráfego

Tráfego de dados	**Drones**					
	Parrot Bebop		DBPower UDI		DJI Spark	
Bidirecional	Dataset 1	Data_te: 17629x55 Data_tr: 1751x55	Dataset 2	Data_te: 15687x55 Data_tr: 1569x55	Dataset 3	Data_te: 5000x55 Data_tr: 500x55
Unidirecional	Dataset 4	Date_te: 10600x19 Data_tr: 1063x19	Dataset 5	Data_te: 13513x19 Data_tr: 1351x19	Dataset 6	Data_te: 66x19 Data_tr: 7x19

Os conjuntos de dados estão divididos assim: conjunto de treinamento $data\_tr$, conjunto de teste $data\_te$, e última coluna com rótulo 1, significando VANT ou 0, caso contrário. Estes conjuntos estão distribuídos em matrizes de objetos X_{nd}, em que n é o número de objetos e d é o número de atributos de entrada de cada objeto. Todos os atributos de entrada são medidas estatísticas calculadas a partir dos dados brutos.

3.2. Caracterização dos Dados

Para todos os conjuntos de dados, os tamanhos dos pacotes e o tempo entre as chegadas destes pacotes são as fontes de dados brutos, pois os demais atributos presentes em pacotes são qualitativos nominais e agregam pouca informação para resolução do problema (dados brutos não disponibilizados).

Para cada fonte, o autor realizou a extração de 9 atributos estatísticos referentes aos tamanhos dos pacotes (*size*) e aos intervalos de tempo (*interval*) entre a transferência de dois pacotes e os disponibilizou nas bases de dados [Zhao 2018]. Para aqueles baseados em fluxo bidirecional, dados referentes a fluxos *uplink*, *downlink* e total (*both_links*) são considerados, enquanto que, para aqueles baseados em fluxo unidirecional, apenas o tráfego em uma direção (*uplink*) é considerado. A Tabela 2 descreve os dados estatísticos empregados para gerar os atributos do conjunto de dados.

Tabela 2. Atributos dos dados gerados a partir dos dados brutos [Zhao L. and K. 2018].

Atributos	Descrição
V1	Média
V2	Mediana
V3	Desvio absoluto mediano
V4	Desvio padrão
V5	Obliquidade

Atributos	Descrição
V6	Curtose
V7	Valor máximo
V8	Valor mínimo
V9	Quadrado médio

Portanto, os três primeiros conjuntos de dados de fluxo bidirecional (*datasets* 1,2 e 3) apresentam 9 atributos de 2 fontes resultantes de 3 direções de fluxos (*uplink*, *downlink* e *both_links*), totalizando 54 atributos de entrada. Já para o fluxo unidirecional (datasets 4,5 e 6) há 9 atributos estatísticos referentes aos tamanhos dos pacotes de informação (*uplink_size*) e aos intervalos de recebimento (*uplink_interval*), totalizando 18 atributos.

Cada objeto contém um atributo alvo qualitativo nominal binário: 1 (existência de intruso) ou 0 (sem intruso), logo esta se caracteriza como uma tarefa preditiva de classificação binária. Os conjuntos de dados já estão amostrados e separados para treinamento e para teste. Nas próximas seções, usaremos a seguinte notação para indicar se um atributo estatístico corresponde ao tamanho do pacote de informação (*uplink_size*) ou ao intervalo de tempo (*uplink_interval*): V_i+ *size* ou V_i+ *inter*, com $i \in [1, 2, 3...9]$.

3.3. Técnicas

O problema abordado irá utilizar técnicas de aprendizado de máquina para tarefas preditivas supervisionadas de classificação, sendo esta uma classificação binária. Portanto a saída de nosso classificador é um indicador da natureza do trafego (VANT ou não), configurando assim em uma tarefa de classificação.

4. Experimentos e Resultados

A seguir, serão descritos os experimentos utilizados na exploração de dados, pré-processamento e geração dos modelos preditivos.

4.1. Exploração dos Dados

Neste projeto, foi realizado um recorte do problema de classificação, de modo a inicialmente simplificar o problema. Logo, foi estabelecido como foco o uso dos dados dos *Datasets 4,5 e 6* a fim de concentrarmos nossa análise no estudo da classificação de objetos referentes a fluxos unidirecionais de informações.

Na etapa de análise exploratória, a concatenação dos *Datasets 4,5 e 6* foi realizada e, em seguida, foi possível confirmar a inexistência de dados ausentes. A junção desses *datasets* resultou em um conjunto com um total de 26.600 objetos que possuem um total de 18 atributos quantitativos racionais e 1 atributo alvo binário que indica se o objeto pode ou não ser classificado como um VANT (1 para VANT e 0 caso contrário). Ademais, a checagem do balanceamento dos dados demonstrou que a classe dominante denotada por 1, correspondente à classe VANT, representa $53,3\%$ dos dados. Medidas de localidade, espalhamento e distribuição dos dados encontram-se relacionadas nas Tabelas 3 a 5.

Tabela 3. Atributos referentes aos tamanhos dos pacotes de informação.

Atributo / Dado	V1 *size*	V2 *size*	V3 *size*	V4 *size*	V5 *size*	V6 *size*	V7 size	V8 *size*	V9 *size*
média	0.1413	0.8321	0.0092	0.0054	4.0116	23.1255	7.5087	0.0001	0.845
desvio padrão	2.3531	21.3945	0.5917	0.0485	2.2606	23.7243	213.352	0.0001	21.4168
min	0.0001	0.0	0.0	0.0	-1.9319	-1.9807	0.0002	0.0	0.0001
25%	0.0013	0.0025	0.0001	0.0001	2.3231	5.7673	0.0166	0.0	0.0029
50%	0.0033	0.0082	0.0003	0.0002	3.4637	13.738	0.0477	0.0	0.0093
75%	0.0122	0.0267	0.0009	0.0008	5.4842	33.71	0.1515	0.0001	0.0289
max	149.87	1492.4	68.171	3.9419	9.8493	98.01	14925.0	0.0082	1492.5

Tabela 4. Atributos referentes aos intervalos de transferência entre pacotes de informação.

Atributo / Dado	V1 *inter*	V2 *inter*	V3 *inter*	V4 *inter*	V5 *inter*	V6 *inter*	V7 *inter*	V8 *inter*	V9 *inter*
média	746.754	351.673	863.5097	97.517	-0.5053	4.6564	1121.2766	167.1006	842.8334
desvio padrão	514.2398	264.5077	657.7561	192.386	2.2341	14.1061	658.1798	151.6565	550.8321
min	63.52	0.2	62.0	0.0	-9.702	-2.0199	68.0	61.0	63.981
25%	123.1475	40.376	138.0	0.0	-1.0159	-1.2723	183.0	76.0	130.64
50%	866.255	359.49	1166.0	0.0	-0.3316	1.1759	1502.0	76.0	1083.4
75%	1141.125	618.95	1476.0	112.68	0.5807	2.249	1610.0	222.0	1285.5
max	1675.7	761.07	1676.0	1136.4	9.8494	98.01	3468.0	1676.0	1675.7

Tabela 5. Valores de obliquidade e curtose dos atributos.

Atributo		**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
Obliquidade	***Size***	42.3114	48.1196	114.9621	47.2162	0.7266	1.3725	48.4269	20.7556	48.016
	Inter	0.0228	0.0022	-0.0752	2.707	-0.8213	4.4754	-0.7094	3.9658	-0.2779
Curtose	***Size***	1986.326	2558.709	13242.3318	3410.116	-0.218	1.013	2585.214	979.722	2549.395
	Inter	-1.367	-1.615	-1.823	7.93	4.768	22.253	-1.406	24.735	-1.531

Observando os valores das tabelas acima, podemos constatar grandes diferenças entre as médias, os desvios padrão e as medidas de distribuição dos atributos. Particularmente, pode-se notar que os atributos referentes aos intervalos entre os pacotes (demonstrados na Tabela 4) possuem, em geral, desvios padrão consideravelmente maiores do que os referentes aos tamanhos deles (presentes na Tabela 3). Certamente, isso reflete-se nos gráficos de *scatter plot* demonstrados nas Figuras 3 e 4, que evidenciam maiores espalhamentos dos pontos na segunda figura.

A Tabela 5 denota que os atributos referentes aos tamanhos possuem obliquidades mais positivas e, portanto, eles têm distribuições mais concentradas para o lado esquerdo, fato que também é confirmado na Figura 3, onde pode-se notar distribuições mais voltadas para a esquerda. Ademais, os valores de curtose na Tabela 5 denotam que os atributos relacionados ao tamanho possuem distribuições mais altas e concentradas do que a distribuição normal, enquanto que esse efeito é menos acentuado nos atributos referentes aos intervalos (neles, a maioria dos valores de curtose é negativa e, portanto, as distribuições desses dados são mais achatadas que a normal).

Além disso, nos gráficos 3 e 4, (onde, em verde, destacam-se objetos correspondentes a VANTs e, em azul, não VANTs) podem-se observar correlações entre alguns atributos. Os pares de atributos que possuem correlações mais evidentes e que mais se aproximam de relações lineares são V_1 *size* e V_2 *size*, V_1 *size* e V_7 *size*, V_1 *size* e V_9 *size*, V_2 *size* e V_7 *size*, V_2 *size* e V_9 *size*, V_7 *size* e V_9 *size*, V_1 *inter* e V_9 *inter*.

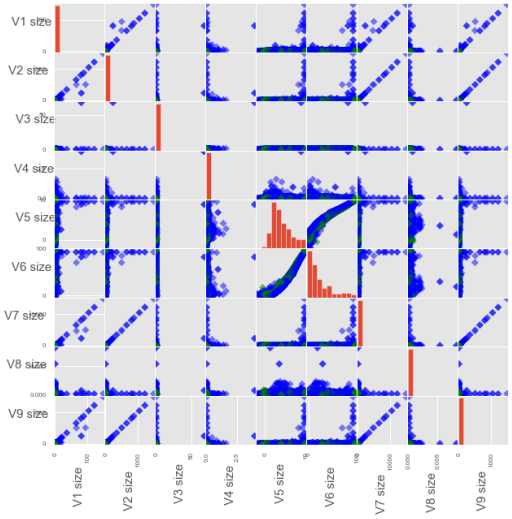

Figura 3. Distribuições dos dados - tamanhos dos pacotes.

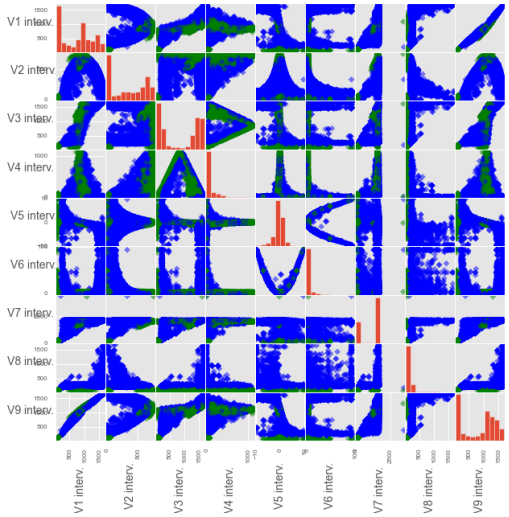

Figura 4. Distribuições dos dados - intervalos entre pacotes.

A fim de observar as correlações entre os atributos, foram construídos os *heatmaps* da Figura 5, que demonstram os coeficientes de correlação de Pearson e de Spearman. Observando-os, constata-se que, de fato, as medidas de tendência central (V_1 *size* e V_2 *size*) e formato das distribuições (V_5 *size* e V_6 *size*) são fortemente correlacionadas nos dados referentes aos tamanhos dos pacotes. Este mesmo tipo de correção só existe nas medidas de tendência central referentes aos intervalos entre pacotes (V_1 *inter* e V_2 *inter*), sendo que (V_1 *inter* é mais correlacionada com V_3 *inter*) e V_9 *inter*), o que mostra a diferença de distribuição entre as dois dados bases dos atributos usados. Por fim, constatou-se que as medidas de máximo V_7 *size* e V_7 *inter* são fortemente correlacionadas com as métricas de quadrado médio V_9 *size* e V_9 *inter*, respectivamente. Essas análises serão úteis na etapa de pré-processamento relacionada com a verificação de importância de cada atributo.

4.2. Pré-processamento dos Dados

Inicialmente, buscou-se a existência de atributos redundantes, como resultado foram identificados um total de 3419 elementos duplicados. A eliminação desses dados resultou em uma base de dados com 23181 objetos, com 61.1% pertencentes à classe VANT, evidenciando um maior desbalanceamento.

Para lidar com este desbalanceamento resultante, utilizou-se a técnica *random undersampling*, que permite retirar aleatoriamente dados da classe majoritária e assim, balancear os dados. Após aplicação do *undersampling*, o conjunto de dados decorrente passou a conter 9010 elementos em cada classe (VANT e não-VANT).

Após a eliminação de dados redundantes e balanceamento, foi realizada a padronização do conjunto de dados. Essa escolha foi motivada pelas observações realizadas anteriormente, que demonstraram a existência de medidas de escala e de espalha-

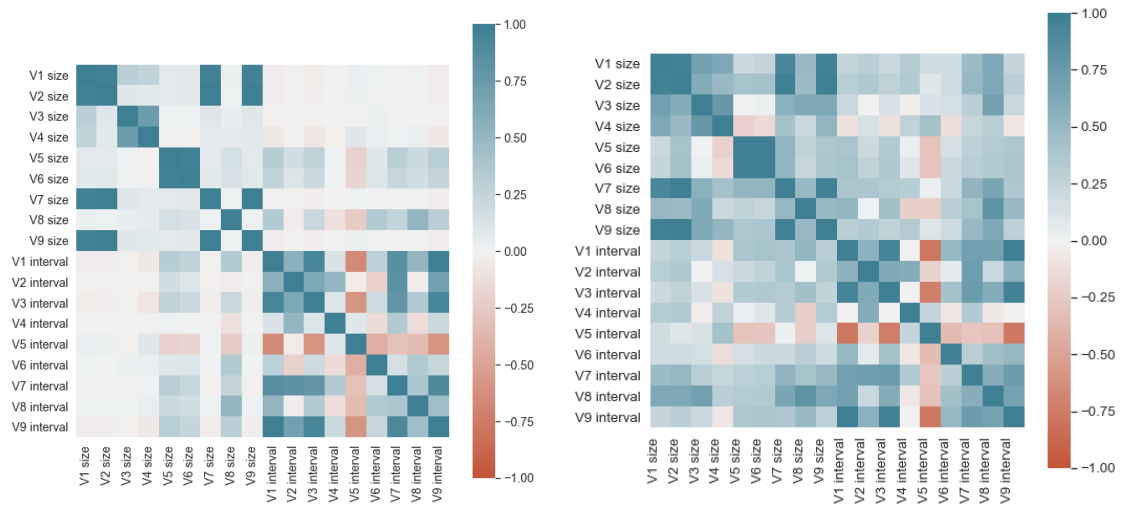

Figura 5. Gráficos do tipo *Heatmap*, de correlações entre os atributos. À esquerda, correlações de Pearson e, à direita, correlações de Spearman.

mento desiguais. Como alguns modelos não lidam bem com dados não padronizados, essa medida foi aplicada a *priori*. Além disso, a normalização por padronização lida melhor com possíveis *outliers* quando comparada com a normalização por reescala [Faceli 2021].

A fim de reduzir o custo computacional da etapa de treinamento e evitar problemas relacionados à ”maldição da dimensionalidade”, como *overfitting*, por exemplo, decidiu-se realizar uma seleção dos atributos, identificando e descartando aqueles que sejam irrelevantes ou redundantes. Para isso, foram utilizados critérios subjacentes a duas técnicas: análise de variância (ANOVA) e informação mútua (*Mutual Information*) [Witten 2011].

Aplicando as técnicas acima descritas, chegou-se à seleção de 10 atributos: V1 *size*, V4 *size*,V5 *size*, V8 *size*, V1 *inter*, V3 *inter*, V6 *inter*, V7 *inter*, V8 *inter* e V9 *inter*. Contudo, quando tentou-se avaliar o efeito dessa seleção por meio do uso de um conjunto de classificadores, constatou-se acurácias e precisões superiores a 99,9% em todos os modelos obtidos, chegando a 100% com Árvore de Decisão e SVM linear.

Nesse contexto, verificou-se que o atributo V8 *inter* possui importância consideravelmente maior que os demais, uma vez que por foi analisada as pontuações de importância das *features* na árvore de decisão com base no critério Gini [Faceli 2021]. A partir disso, pôde-se concluir que a base de dados possui um forte viés neste atributo, o que configuraria um caso de *feature bias* resultante, provavelmente fruto do processo de geração da base de dados. Diante disso, optou-se por utilizar a normalização por reescala (atributos com valores entre 0 e 1) e, em seguida, desconsiderou-se atributos com variância inferior a $0,1$. Isso se justifica pelo fato de que, primeiramente, a normalização por reescala é essencial para a obtenção de predições representativas em algoritmos baseados em distâncias. Ademais, verificou-se que, ao se aplicar o filtro de variância supracitado, pôde-se eliminar o atributo V8 *inter* e outros cujas variâncias demonstraram pouca representatividade. Assim, pôde-se tratar simultaneamente problemas relacionados ao viés correspondente a uma das *features* e à presença de atributos pouco representativos. A partir disso, os atributos selecionados foram V1 *inter*, V2 *inter*, V3 *inter* e V9 *inter*.

4.3. Geração de modelos de AM

Na etapa de geração de modelos, foram explorados os seguintes classificadores: Regressão Logística (LR) Algoritmo de k Vizinhos mais Próximos (k-NN), Árvores de Decisão (AD), Floresta Aleatória (RF), Redes Neurais Artificiais (*Multi Layer Perceptron* - MLP), *Support Vector Classifier* (SVC), *Gaussian Naïve Bayes* (GNB) e *AdaBoost*. Na tabela 6, verificam-se as médias e os desvios-padrão (D.P.) das seguintes métricas de desempenho dos classificadores: acurácia, precisão, revocação e medida-F1. Nesse cenário, o método de amostragem de dados empregado para a geração e avaliação dos modelos preditivos foi a validação cruzada estratificada com 10 partições.

Tabela 6. Desempenho dos classificadores para cada métrica, Tempo de predição em segundos e melhor classificador

		LR	*SVC*	*AD*	*RF*	*GNB*	*AdaBoost*	*k-NN*	*MLP*	*Melhor*
Acurácia	*Média*	0.8193	0.9217	0.9628	0.9925	0.6048	0.8469	0.9914	0.9647	Random Forest
	D.P	0.0635	0.0130	0.0085	0.0023	0.0717	0.0973	0.0030	0.0085	
Precisão	*Média*	0.7710	0.9050	0.9459	0.9898	0.6407	0.7891	0.9895	0.9606	Random Forest
	D.P	0.0833	0.0229	0.0120	0.0040	0.1195	0.1051	0.0049	0.0139	
Revocação	*Média*	0.9273	0.9431	0.9819	0.9952	0.5385	0.9836	0.9933	0.9693	k-NN
	D.P	0.0067	0.0048	0.0103	0.0023	0.0125	0.0067	0.0026	0.0061	
F1 Score	*Média*	0.8396	0.9235	0.9635	0.9925	0.5802	0.8713	0.9914	0.9649	Random Forest
	D.P	0.0490	0.0120	0.0083	0.0022	0.0454	0.0676	0.0029	0.0083	
Tempo de predição	*Média*	0.0124	0.5393	0.0119	0.0555	0.0124	0.0216	0.1570	0.0159	Árvore de decisão
	D.P	0.0021	0.2368	0.0029	0.0078	0.0048	0.0075	0.0524	0.0038	

A métrica de avaliação utilizada para a seleção de modelos foi a precisão, uma vez que, pela natureza do problema, é preferível a classificação de todos os intrusos, ainda que alguns deles sejam falsos. Nesse caso, é possível garantir maior segurança ao identificar todos os possíveis intrusos mesmo com o custo de se detectar alguns sendo falsos positivos. Além disso, também fez-se uso das curvas ROC (*Receiving Operating Characteristics*) para avaliar os classificadores. Estas demonstram as variações das taxas de verdadeiros positivos com as de falsos positivos em diferentes valores de limiares (*thresholds*) utilizados para determinar as classificações. Nesse contexto, quanto maior a área abaixo da curva (AUC), melhor é o desempenho preditivo do classificador.

Por fim, com o objetivo de investigar a ocorrência de *overfitting*, foram construídas as curvas de aprendizado demonstradas na Figura 6. Elas tiveram como foco a análise dos três modelos que atingiram maiores valores de AUC.

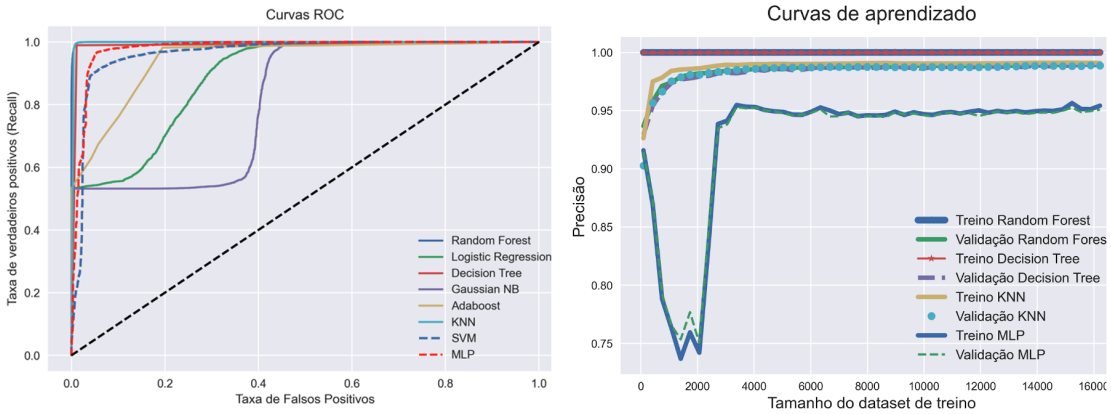

Figura 6. Curvas ROC (à esquerda) e curvas de aprendizado dos preditores obtidas através de treinamentos com *datasets* de diferentes tamanhos (à direita).

5. Discussão

Nota-se pela tabela 6 que o melhor modelo preditivo obtido, em termos de acurácia e precisão, foi com o método *Random Forest*, demonstrando ser um algoritmo muito competitivo neste contexto, porém com custo computacional elevado para predição. Destaca-se que o método de AD apresentou a menor latência para predição, cerca de 5 vezes menor a RF.

Também a partir da tabela 6, observa-se que os preditores que atingiram maiores precisões foram *Random Forest*, k-NN, AD e MLP. Além disso, esses foram os modelos que apresentaram maiores valores de AUC (0,999, 0,997 ,0,988 e 0.979 respectivamente), portanto, apresentaram melhor desempenho na distinção entre as classes. Logo, estes foram os algoritmos utilizados na analise das curvas de aprendizado da Figura 6 com o objetivo de direcionar a analise dos melhores modelos. Vale ressaltar que, conforme [Zhao L. and K. 2018], precisões acima de 90% são desejáveis nesse contexto e, por isso, deu-se preferência a modelos com precisões dessa ordem.

A convergência dos modelos para índices elevados de desempenho denotam a possibilidade de ocorrência de *overfitting* nos dados, de modo que eles podem ser pouco generalizáveis para os diversos dispositivos e aplicações conectadas à rede. Diante disso, ressalta-se a importância da análise da Curva de Aprendizado, que verifica a mudança da precisão do modelo com o aumento do número de amostras. Analisando-as, constata-se a existência de um *gap* entre as curvas de treino e de validação dos modelos *Random Forest* e *Decision Tree*. Isso representa uma tendência tipica de *overfitting*, quando as performances de treino superam consideravelmente às de validação. Por isso, o modelo MLP possivelmente seria uma boa escolha neste contexto, pois apresenta um bom *trade-off* entre precisão (96%), baixo tempo de resposta e variação, com ausência de traços de *overfitting*.

Já o modelo obtido com GNB apresentou o pior desempenho, dado ao fato do método ter a premissa de independência entre atributos, o que não acontece, visto que temos a geração de atributos a partir dos demais, por exemplo V3 *inter* necessita de V2 *inter* (desvio absoluto mediano e mediana). O modelo de SVC, que também faz o uso de ferramentas estatísticas, exibiu desempenho reduzido em comparação aos demais com elevado tempo de predição (45 vezes maior que AD).

6. Conclusão

Neste projeto objetivou-se a identificação de Drones invasores com o uso de técnicas preditivas supervisionadas de classificação binária de aprendizagem de máquina por meio de dados de sinais wi-fi criptografados, isto é, com base no tamanho e tempo de intervalos entre os pacotes de dados. Adota-se a precisão como métrica para o problema dessa classificação, para a maior segurança na detecção dos invasores, mesmo que apresentem falsos positivos. Porém nota-se que é interessante levar em conta o *trade-off* de precisão e tempo de execução de previsão do método, visto que os intrusos voam a altas velocidades.

Iniciou-se com uma exploração e posterior pré processamento dos dados, e logo a redução de atributos para se evitar problemas decorrentes de grande dimensionalidade. Além disso, utilizou-se um filtro de variância aos dados normalizados para mitigar o possível viés do atributo alvo na base de dados, resultando em quatro atributos resultantes,

todos relativos ao intervalo entre pacotes. Durante o decorrer das analises, foi identificado um forte viés na predição com o uso do atributo V8 *inter*, exibindo um desempenho preditivo de 100% com AD com apenas uma regra e altos índices com a maioria dos demais modelos (99.9% de precisão e acurácia). A solução encontrada foi a remoção a partir do filtro de variância, já que este apresentava variância reduzida. Porém levanta-se dúvidas sobre qualidade da coleta desta base de dados, dado este viés e a seleção de apenas atributos de intervalo como representativos.

Da análise dos modelos preditores, houve precisão na faixa de 64,07% até 99,52%. O melhor modelo em questão de precisão e acurácia foi RT, porém com tempo de predição elevado. Chega-se a um melhor balanceamento entre precisão e tempo com a rede MLP, demonstrando elevada precisão (96,06%), predição em 0.0159s com baixa variância e ausência de identificação de *overfitting*. Conclui-se que a aplicação de métodos de AM nesse contexto é promissor, porém devido a base de dados apresentar viés, o que levantou dúvidas da qualidade da base de dados, assim que são necessário novos estudos experimentais com maior variabilidade de dados de distintos drones e demais dispositivos.

Referências

Witten, I. H. (2011). Data mining : practical machine learning tools and techniques.— 3rd ed. Elsevier.

Boyle, M. G. (2015). The race for drones. In *Foreign Policy Research Institute*. E-Notes.

Vattapparamban, E.; Guvenc, E. Y. A. A. K. and Uluagaç, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. Department of Electrical Eng. - FIU, Miami, FL, USA.

Zhao, L. (2018). Unmanned aerial vehicle (uav) intrusion detection datasets. disponível em: `http://mason.gmu.edu/~lzhao9/materials/data/UAV/` . acesso em: 01/04/21.

Ulrich, P. H. and Nobre, J. C. (2019). Análise do estado da arte em segurança cibernética com drones. Universidade do Vale do Rio dos Sinos (UNISINOS).

Schroth, L. (2020). The drone market size 2020-2025: 5 keys takeaways. disponível em: `https://droneii.com/the-drone-market-size-2020-2025-5-key-takeaways` . acesso em: 01/04/21.

Alipour-Fanid, A.; Wang, N. and Zhao, L. (2020). Machine learning-based delay-aware uav detection and operation mode identification over encrypted wi-fi traffic. IEEE Transactions on Information Forensics and Security.

Faceli, K.;Lorena, A. C. G. J. C. A. C. P. L. F. (2021). Inteligência artificial: Uma abordagem de aprendizado de máquina. Editora LTC.

Zhao L., Alipour-Fanid A., S. M. and K., Z. (Aug 2018). Prediction-time efficient classification using feature computational dependencies. Proceedings of the 24st ACM SIGKDD Conference on Knowledge Discovery and Data Mining.

Gharibi, M., B.-R. and Waslander, S. (Fev. 2016). Internet of drones. IEEE Access.

Altawy, R. and Youssef, A. M. (Nov 2016). Security, privacy, and safety aspects of civilian drones: A survey. In *ACM Trans*. Cyber-Phys. Syst. 1, 2, Article 7.