ISSN: 1983 7402 ITA, 28 a 29 SET 2021

Detecção de Drones Intrusos

Livia Fragoso Pimentel[1], Luiz C. Giacomossi Jr.[1], Jefferson Costa de Matos [1,2], Vitor Venceslau Curtis[1], Filipe Alves Neto Verri[1]

[1]Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil
[2]Universidade Federal de São Paulo (UNIFESP), São José dos Campos/SP – Brasil

***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 à 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 deles e da avaliação de modelos preditivos com o objetivo de selecionar aqueles capazes de prover maiores precisões e menores tempos de processamento ao classificar se um sinal é proveniente de um drone, ou não.**

***Palavras-Chave* – Drone, Aprendizado de Máquina, Detecção.**

I. INTRODUÇÃO

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 (*last mile delivery*), inspeções técnicas em locais de difícil acesso e operações militares. 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 [1] [2].

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 da privacidade. No Brasil, como a regulamentação do uso desses veículos ainda é incipiente, algumas restrições práticas se apresentam como, por exemplo, a impossibilidade de utilizá-los largamente em regiões próximas a centros urbanos.

Como destacado, o aumento de VANTs suscita questões acerca dos riscos potenciais para a segurança pública e para a privacidade pessoal. Para minimizá-los, detectar e identificar com eficiência VANTs invasores é uma necessidade urgente. Os métodos de detecção física existentes (como radar, visão e som) podem ser ineficazes em alguns cenários: por exemplo, sinais de radar podem ser bloqueados por obstáculos, especialmente em ambientes civis. Para contornar esses problemas, uma solução promissora para a detecção de drones invasores é o uso de modelos preditivos capazes de analisar esses dados e aprender características típicas de sinais provenientes de drones.

Diante desse cenário, pretende-se aplicar técnicas de aprendizagem de máquina para detecção de drones intrusos, explorando os dados existentes provindos de sinais wi-fi criptografados de VANTs comerciais.

Livia Fragoso Pimentel, livia.pimentel@ga.ita.br; Luiz C. Giacomossi Jr., luiz.giacomossi@ga.ita.br; Jefferson Costa de Matos, dematos@ita.br; Vitor Venceslau Curtis, curtis@ita.br; Filipe Alves Neto Verri, verri@ita.br

Em uma análise prévia, constata-se que é possível aplicar técnicas de aprendizagem supervisionada, uma vez que o problema em questão se trata de uma tarefa preditiva de classificação binária. Ademais, além da precisão dessa classificação, o tempo de execução da classificação também é importante, visto que os intrusos voam a uma velocidade considerável. Portanto, é necessário otimizar em conjunto o tempo de execução da previsão e sua precisão nesse contexto.

Este artigo é constituído de um breve referencial teórico sobre o tema (Seção II), seguido da Seção III, onde serão descritos os métodos e as técnicas usadas no tratamento e na caracterização dos dados. A seção IV é dedicada aos experimentos aos quais a base de dados foi submetida, para a posterior aplicação e avaliação de modelos preditivos. Por fim, na parte V, encontram-se discussões acerca dos resultados obtidos e, em seguida, a conclusão será apresentada.

II. BIBLIOGRAFIA CORRELATA

Diversos estudos focam nos desafios enfrentados no controle de drones visando à manutenção da privacidade e da inviolabilidade da propriedade privada, bem como aspectos éticos de seu uso, abordando aspectos jurídicos e de costume [3]. 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 [4]. Neste paper, além da revisão sobre segurança cibernética com VANTs, analisam-se as ferramentas de comando, controle e comunicações.

Em [5], os autores fazem uma proposta para identificação de drones intrusos considerando um ambiente comumente chamado na área de Internet de Drones (IoD). Nesse contexto, os dados seriam transmitidos entre o drone e a estação terrestre de controle, de forma que os dados suspeitos, isto é, potencialmente não autorizados, seriam armazenados em uma *blockchain* privada, permitindo assim um registro e análise do sistema de segurança com os dados de vôos.

Com relação à integração de drones em cidades, os mecanismos de bloqueios de VANTs em áreas perigosas e não autorizadas também representam temas oportunos. Nesse contexto, [6] apresenta sistemas de interrupção de drones intrusos por meio de diversas técnicas como, por exemplo, o emprego de aves treinadas para capturas e interrupção através de outros drones, não focando, contudo, no problema de detecção. Neste trabalho são citando não somente as ameaças de usos de drones, como também aplicações benéficas da ferramenta, como em resgates, perícias, etc.

Exemplos de uso de aprendizado de máquina para identificar drones por sinais wi-fi e rádio frequência (RF) são vistos em [7] e [8]. Nesses trabalhos, os modelos podem detectar atividade de drones no espectro de RF a partir de parâmetros como os tamanhos dos pacotes de mensagens, espaços de tempo entre elas e outros parâmetros estatísticos.

Porém, mais trabalhos são necessários para aprimorar a detecção para que possam ser empregados de forma prática.

III. MATERIAIS E MÉTODOS

Neste projeto, a manipulação dos dados e a geração de modelos preditivos foram realizados por meio da biblioteca *Scikit-learn*, da linguagem Python. A seguir, serão detalhados os métodos e as ferramentas utilizados neste estudo com o objetivo de construir e avaliar modelos gerados para a detecção de drones intrusos.

A. Conjunto de Dados

Para a detecção VANTs intrusos foram utilizados o conjunto de dados disponibilizado em [9]. 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. Pode haver vários usuários de wi-fi na faixa de detecção, sendo estes VANTs ou dispositivos não-VANTs, como computadores e celulares.

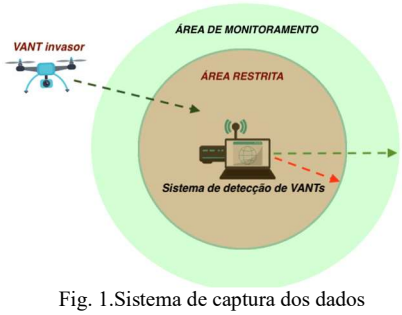


Fig. 1.Sistema de captura dos dados

Este sistema de detecção, descrito na Fig. 1, captura pacotes de dados (criptografados e não-criptografados) dentro de uma área delimitada, com o uso do software *opensource* WireShark [10]. 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, que consiste em um conjunto de características estatísticas calculadas a partir dos dados brutos de rede. Seguindo esta ideia, seis conjuntos de dados reais para detecção de intrusos estão disponíveis. 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 Fig. 2.

Fig. 2 Drones comerciais utilizados [10].

Assim, estes conjuntos de dados são combinações entre os diferentes tipos de VANTs e modos de tráfego dos dados descritos na Tabela I.

TABELA I - CONJUNTOS DE DADOS DOS DRONES COMERCIAIS

Modo de tráfego	**Drones**					
	Parrot Bebop		***DBPower***		***DJI Spark***	
Bidirecional	I	Data te: 17629x55	II	Data te: 15687x55	III	Data te: 5000x55
		Data tr: 1751x55		Data tr: 1569x55		Data tr: 500x55
Unidirecional	IV	Date te: 10600x19	V	Data te: 13513x19	VI	Data te: 66x19
		Data tr: 1063x19		Data tr: 1351x19		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 *Xnd*, em que *n* é o número de objetos e *d* representa o número de atributos de entrada de cada objeto. Todos os atributos de entrada são medidas estatísticas calculadas a partir dos dados brutos.

B. 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 [10]. 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 II descreve os dados estatísticos empregados para gerar os atributos do conjunto de dados.

TABELA II - ATRIBUTOS DOS DADOS GERADOS A PARTIR DOS DADOS BRUTOS [9].

Atributo	**Descrição**	**Atributo**	**Descrição**
V1	Média	V6	Curtose
V2	Mediana	V7	Valor máximo
V3	Desvio absoluto mediano	V8	Valor mínimo
V4	Desvio padrão	V9	Quadrado médio
V5	Obliquidade		

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 (caso contrário), 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* pertencendo ao seguinte intervalo [1, 2, 3...9], de acordo com a representação descrita na Tabela II.

C. 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 tráfego (VANT ou não), configurando assim em uma tarefa de classificação.

IV. EXPERIMENTOS E RESULTADOS

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

A. 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 a classe VANT, representa 53,3% dos dados. Medidas de localidade, espalhamento e distribuição dos dados foram avaliadas nos *boxplots* da Fig. 3 e da Fig. 4.

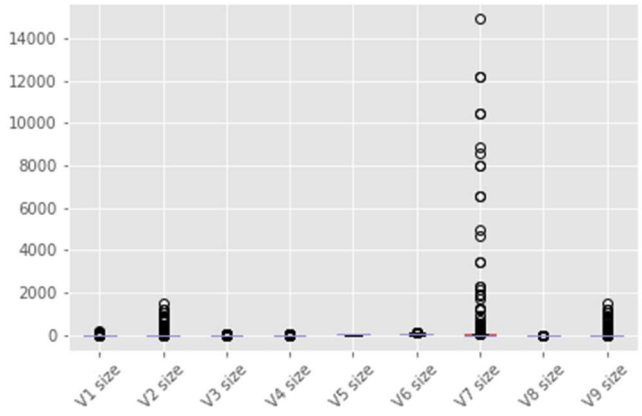


Fig. 3. *Boxplots* dos atributos relacionados aos tamanhos dos pacotes de informação.

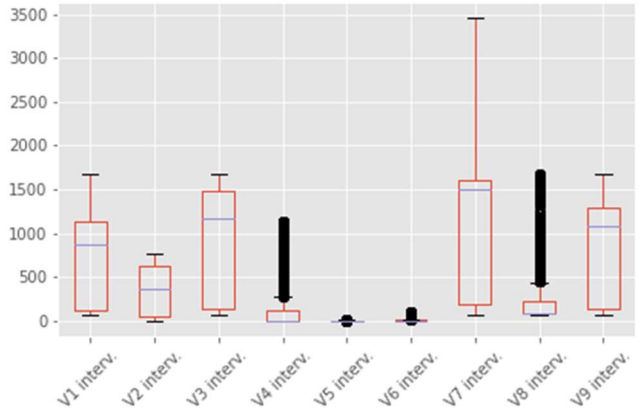


Fig. 4. *Boxplots* dos atributos relacionados aos tamanhos dos intervalos entre pacotes de informação.

Observando os perfis dos *boxplots*, 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 possuem, em geral, desvios padrão consideravelmente maiores do que os referentes aos tamanhos deles. Certamente isso reflete-se nos gráficos de *scatter plot* demonstrados na Fig. 5 e na Fig. 6, que evidenciam maiores espalhamentos dos pontos na segunda figura.

Observando os gráficos da Fig. 5 e da Fig. 6, também pode-se perceber que os atributos referentes aos tamanhos possuem distribuições mais concentradas para o lado esquerdo. Ademais, percebe-se que esses atributos 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, nessas figuras (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 *V1 size* e *V2 size*, *V1 size* e *V7 size*, *V1 size* e *V9 size*, *V2 size* e *V7 size*, *V2 size* e *V9 size*, *V7 size* e *V9 size*, *V1 inter* e *V9 inter*.

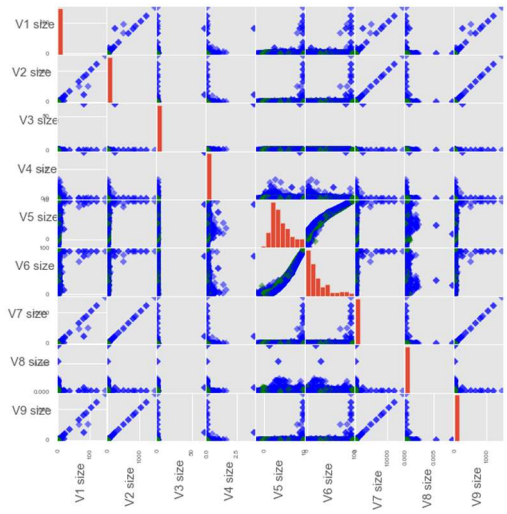


Fig. 5. Distribuições dos dados - tamanho dos pacotes.

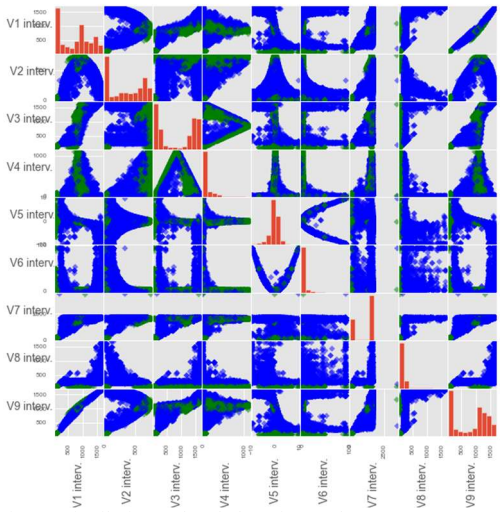


Fig. 6. Distribuições dos dados - intervalo entre pacotes.

A fim de analisar quantitativamente as correlações entre os atributos, foi construído o *heatmap* da Fig. 7, que demonstra os coeficientes de correlação de Pearson entre eles. Nesse contexto, constata-se que, de fato, as medidas de tendência central (*V1 size* e *V2 size*) os formatos de distribuições (*V5 size* e *V6 size*) são fortemente correlacionadas linearmente nos dados referentes aos tamanhos dos pacotes. Este mesmo tipo de correlação são existe nas medidas de tendência central referentes aos intervalos entre pacotes (*V1 inter* e *V2 inter*), sendo que *V1 inter* é mais correlacionada com *V3 inter* e *V9 inter*, o que mostra a diferença de distribuição entre os dois dados bases dos atributos usados. Por fim, constatou-se que as medidas de máximo *V7 size* e *V7 inter* são fortemente correlacionadas com as métricas de quadrado médio *V9 size* e *V9 inter*, respectivamente. Essas análises serão úteis na etapa de pré-processamento relacionada com a verificação da importância de cada atributo.

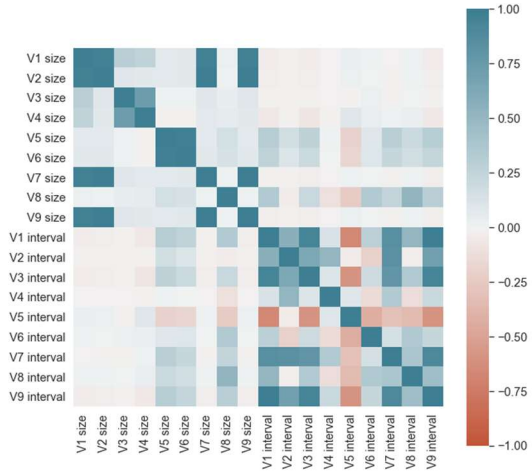


Fig. 7. Gráfico do tipo *Heatmap*, que demonstra correlações de Pearson entre os atributos.

B. Pré-processamento dos Dados

Inicialmente, buscou-se verificar a existência de dados redundantes e, como resultado, foram identificados um total de 3.419 elementos duplicados. A eliminação desses dados resultou em uma base de dados com 23.181 objetos, com 61,1% deles 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 9.010 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 espalhamento 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 [11].

A fim de reduzir o custo computacional da etapa de treinamento e evitar problemas relacionados à "maldição da dimensionalidade", como o *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*) [12].

Aplicando as técnicas acima descritas, chegou-se a 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 desta 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, através

da análise das pontuações que demonstram a importância das *features* em uma Árvore de Decisão com base no critério Gini [12]. A partir disso, pode-se concluir que a base de dados possui um forte viés neste atributo, o que configura um caso de *feature bias*, 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 à 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, pode-se eliminar o atributo *V8 inter* e outros cujas baixas variâncias indicam pouca representatividade. Assim, pode-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*.

C. Geração de Modelos de Aprendizado de Máquina

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 III são apresentadas, por faixa, as médias 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. Os resultados da velocidade preditores por faixa são apresentados na Tabela IV.

Tabela III - Faixa de desempenho dos classificadores

Métricas	**≤ 0.7**	**[0.7-0.9]**	**≥ 0.9**	**Melhor**
Acurácia	GNB	LR, AdaBoost	SVC, AD, RF, k-NN, MLP	RF
Precisão	GNB	LR, AdaBoost	SVC, AD, RF, k-NN, MLP	RF
Revocação	GNB	-	LR, AdaBooot, SVC, AD, RF, k-NN, MLP	k-NN
F1 Score	GNB	LR, AdaBoost	SVC, AD, RF, k-NN, MLP	RF

Tabela IV - Faixa de tempo de predição dos classificadores em segundos

Métrica	**≤0.02**	**[0.02-0.5]**	**≥0.5**	**Melhor**
Tempo de Predição	LR, AD, RF, GNB, MLP	AdaBoost, k-NN	SVC	AD

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 detectar alguns falsos positivos. Além disso, também fez-se uso das curvas ROC (*Receiving Operating Characteristics*) presentes na Fig. 6 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 ˆ *overfitting*, foram construídas as curvas de aprendizado demonstradas na Fig. 7. Elas tiveram como foco a análise dos três modelos que atingiram maiores valores de AUC.

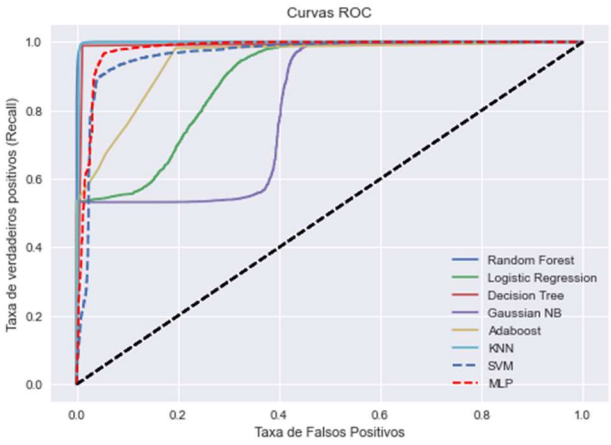
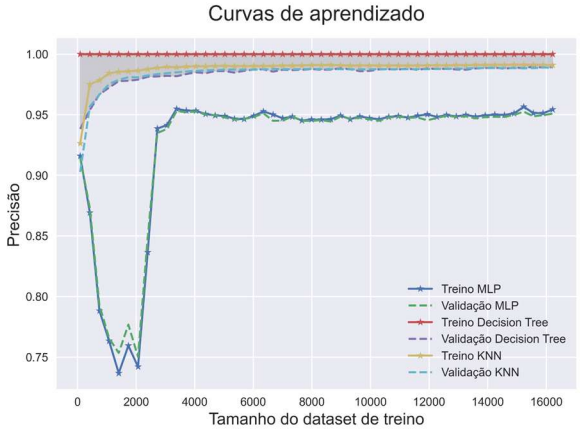


Fig. 6. Curvas ROC (à esquerda) e curvas de aprendizado dos preditores obtidas com *datasets* de diferentes tamanhos (à direita).



V. DISCUSSÃO

Conforme demonstra a Tabela III, o melhor modelo preditivo obtido, em termos de acurácia e precisão, foi o método Floresta Aleatória (RF), que se demonstrou 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 maior que o modelo RF.

Observa-se, também, que os preditores que atingiram maiores precisões foram RF, 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) e, portanto, apresentaram melhor desempenho na distinção entre as classes. Logo, estes foram os algoritmos utilizados na análise das curvas de aprendizado da Fig. 7, com o objetivo de direcionar a análise dos melhores modelos. Vale ressaltar que, conforme [13], precisões acima de 90% são desejáveis nesse contexto e, por isso, deu-se preferência a modelos com indicadores dessa ordem de grandeza.

A convergência dos modelos para índices elevados de desempenho denota a possibilidade de ocorrência de *overfitting* dos 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* pronunciado entre as curvas de treino e de validação dos modelos RF e AD. Isso representa uma tendência típica de overfitting, quando as performances de treino superam consideravelmente as 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 destes indicadores (D.P.), com ausência de traços de *overfitting*.

Já o modelo obtido com GNB apresentou o pior desempenho, dado ao fato de que esse método se baseia na 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). Além disso, o modelo SVC, que também faz o uso de pressupostos estatísticos como o GNB, exibiu desempenho reduzido em comparação aos demais, com elevado tempo de predição (45 vezes maior que AD).

VI. 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, com base no tamanho e nos intervalos entre os pacotes de dados. Adotou-se nesse contexto a precisão como métrica para o problema dessa classificação, para a maior segurança na detecção dos invasores, mesmo que se apresentem falsos positivos. Porém, nota-se que também é interessante considerar o tempo de execução da classificação, de modo que a identificação de um drone intruso em alta velocidade seja realizada em tempo hábil.

As técnicas empregadas neste trabalho tiveram como ponto de partida a exploração e o posterior pré-processamento dos dados, e a seleção de atributos a fim de evitar problemas decorrentes da “maldição da dimensionalidade” como, por exemplo, o *overfitting*. Utilizou-se, nesse caso, um filtro de variância nos dados normalizados para evitar a presença de atributos com baixa variabilidade e, portanto, irrelevantes, resultando em uma base de dados com quatro atributos relativos ao intervalo entre pacotes. Ao longo dessas análises, identificou-se um forte viés relacionado ao atributo *V8 inter*, pois ele exibiu um desempenho preditivo de 100% com AD com apenas uma regra. Além disso, foram observados altos índices de precisão e acurácia na maioria dos demais modelos. A solução encontrada para esse impasse foi a remoção a partir do filtro de variância, já que muitos atributos, inclusive *V8 inter*, apresentaram variância reduzida. Porém levanta-se dúvidas sobre a qualidade da coleta desta base de dados, frente ao forte viés observado e ao fato de que se obteve como resultado uma seleção de apenas atributos relacionados aos intervalos entre pacotes de informação, excluindo aqueles referentes aos tamanhos desses pacotes.

Na análise dos modelos preditivos, verificaram-se precisões entre 64,07% e 99,52%, sendo RF o modelo que apresentou maiores valores dessas métricas, mas demonstrou como ponto negativo um tempo de predição mais elevado. Nesse contexto, observou-se um melhor balanceamento entre precisão e tempo com a rede MLP, que demonstrou elevada precisão (96,06%), tempo de classificação satisfatório (0.0159s), baixa variância e ausência de *overfitting* em sua curva de aprendizado, fenômeno evidente nos modelos AD e RF.

Conclui-se que a aplicação de métodos de Aprendizado de Máquina nesse contexto é promissora, ressalvando-se, contudo, a observação de que é necessário avaliar se a base de dados apresenta viés considerável relacionado aos atributos. Assim, verifica-se que são recomendáveis em futuros estudos correlatos experimentos com maior variabilidade de dados, e com o emprego de distintos drones e demais dispositivos que utilizam dados wi-fi.

REFERÊNCIAS

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

[2] 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 01/04/2021. (6)

[3] 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. (11)

[4] 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).

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

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

[7] 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.

[8] Scheller, Waylon Dustin, "Detecting drones using machine learning" (2017). *Graduate Theses and Dissertations*. *Iowa State University*.

[9] Zhao, L. (2018). Unmanned aerial vehicle (uav) intrusion detection datasets. Disponível em: <http://mason.gmu.edu/~lzhao9/materials/data/UAV/>. Acesso em: 01/04/2021

[10] Wireshark Disponível em: <https://www.wireshark.org/>. Acesso em: 01/04/2021

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

[12] Witten, I. H. (2011). Data mining : practical machine learning tools and techniques.3rd ed. Elsevier. (1)

[13] 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.