SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Review on Unmanned Aerial Vehicles (UAVs) Categorization Using Machine Learning

Nurfathen Najeeya Effendee[1], Aiffah Mohd Ali[1,*], Safiah Zulkifli[1], Mohamad Haniff Junos[1]

[1] School of Aerospace Engineering, Universiti Sains Malaysia (USM), Engineering Campus, 14300 Nibong Tebal, Pulau Pinang, Malaysia

ARTICLE INFO

Article history:
Received 12 June 2025
Received in revised form 8 September 2025
Accepted 5 December 2025
Available online 21 July 2026

Keywords:
Unmanned aerial systems; unmanned aerial vehicles; software-defined radio; machine learning

ABSTRACT

With the rise of Unmanned Aerial Vehicles (UAVs), also known as drones, revolutionary changes have sparked across multiple sectors. Their emergence has ushered in groundbreaking transformations in various fields. However, drones' industry impact is significant, yet their safety concerns call for robust UAVs warning systems. Enhancing detection capabilities in warning systems is essential, particularly considering the frequent disruptions caused by malicious UAVs, making cost-effective early detection methods crucial despite the benefits drones offer. This paper conducts a review on categorizing UAVs using Software-Defined Radio (SDR) combined with machine learning, aiming to create an effective early warning system. The approach involves utilizing machine learning to detect and classify UAVs. This research lays the groundwork for industries to explore cost-effective UAVs categorization, utilizing machine learning and SDR. It offers a commencement for integrating these technologies into various sectors.

1. Introduction

The emergence of Unmanned Aerial Vehicles (UAVs), commonly known as drones, has brought about groundbreaking transformations in various fields in recent years. Nevertheless, while drones have created new opportunities, their irresponsible and unsafe utilization has resulted in numerous perilous incidents. An effective UAVs warning system must be invented to sustain airport safety from disruption as UAV usage grows.

Utilizing UAVs addresses the constraints of the ground-based system by offering improved accessibility, speed, and reliability. These unmanned vehicles have the capability to provide high-resolution photos without cloud interference, benefiting various commercial applications such as agriculture, mining, and monitoring [1]. One approach to enhancing anti-UAV capabilities involves improving the UAV detection systems within existing warning frameworks, with a focus on upgrading some components. In addition to efficiently detecting and classifying threats, developing an affordable warning system is crucial due to the rising prevalence of UAVs, necessitating an escalation in security measures.

A comprehensive overview of UAV-related incidents is presented through a structured Table 1. The purpose of documenting these incidents is to clarify the diverse range of challenges and scenarios

* *Corresponding author. aiffah@usm.my*

associated with UAVs. This compilation serves as a valuable resource for understanding the various contexts in which UAV-related events occur, including unauthorized drone flights, security breaches, and potential risks to safety. Analysing the patterns and characteristics of these incidents will help comprehend the changing environment around UAVs better and will guide effective defences.

Table 1
UAV-related incidents

Reference	Incident Date	Place	Incident
Oren Liebermann [2]	March 2023	Black Sea	A Russian fighter jet forced down a US Air Force MQ-9 Reaper drone over the Black Sea after damaging its propeller. The Russian jet repeatedly flew in front of the drone and dumped fuel on it before colliding with its propeller, causing the US to bring the drone down in international waters.
Guy Delauney [3]	March 2022	Zagreb, Croatia	A military drone crashed in Zagreb at night causing an explosion in the Jarun district. The crash created a crater and scattered debris near student housing, but no one was injured, though a cyclist fell off his bike. Authorities confirmed that Croatia was not targeted, and experts identified the drone as a Soviet-era TU-141 reconnaissance aircraft based on its markings.
Stewart Carr [4]	September 2021	Stansted Airport, United Kingdom	A holiday jet narrowly avoided a collision with a suspected drone, which flew just six feet away at 2,700 feet above ground. The pilot of the Boeing 737, approaching Stansted airport, saw the drone pass several feet from the nose cone but managed to land safely. The incident is one of the closest near-misses recorded in UK airspace.
Matthis Pechtold [5]	March 2021	Frankfurt Airport, Germany	A drone was spotted flying over Frankfurt Airport on a Saturday evening, circling the area several times. Witnesses reported its presence, describing it as having a red flashing light at the center and white lights around it. Authorities are investigating this disruption to air traffic.
Amy Farnworth [6]	June 2020	Darwen, England	A drone flying over Darwen Moor rendered it too dangerous for helicopters to operate and extinguish the fire on the smouldering land, necessitating the helicopter's landing for safety reasons.
Malek Murison [7]	February 2020	Adolfo Suárez-Barajas Airport, Madrid, Spain	Flights at Madrid's international airport was disrupted for over an hour due to possible drone sightings. Spain’s air navigation authority, reported the issue, leading to the diversion of 26 flights before restrictions were lifted. The Transport Ministry closed the airspace around Adolfo Suárez-Barajas airport, and a security committee is investigating the incident. Two airline pilots had reported seeing drones near the airport.

Machine learning has developed from a range of potent techniques within the field of artificial intelligence and has seen widespread application in data mining. This facilitates the system in acquiring beneficial structural patterns and models from training data [8]. In UAV contexts, machine learning has been integrated for tasks such as object detection, intelligent swarm communication, trajectory optimization, enhancing situational awareness, as well as mitigating malicious attacks and countering jamming [9].

This paper presents a review of UAV categorization using machine learning. Section 2 discusses modulation techniques, transmission systems, classification of detection sensors of UAVs and radio frequency interference. The UAV detection using Software-Defined Radio (SDR) with machine learning is explained in Section 3. Discussion and conclusion are given in Section 4.

2. Unmanned Aerial Vehicles (UAVs)

In the present era, Unmanned Aerial Systems (UAS) like UAVs or drones, play a pivotal role in applications such as aerial surveillance, packet delivery, and secure communication. However, in high-risk environments, communication signals between UAVs and ground stations are susceptible to disruptions, potentially resulting in loss or corruption. This vulnerability arises from the threat of cyber-attacks, including jamming and spoofing, which can compromise the integrity and reliability of communication exchanges [10]. The seamless integration of UAS relies heavily on sophisticated modulation techniques, where understanding modulation techniques, transmission systems, and classification of detection sensors becomes paramount to ensure efficient and reliable data transmission.

In the past, early drones, such as the Radioplane OQ-2 developed during World War II, were less advanced than today's UAVs. These drones were controlled using radio signals sent by operators on the ground to control the drone in flight [11]. Drone communication has evolved, and various technologies have been used for communication between drones and their operators. Figure 1 below shows a UAS architecture.

Figure 1 depicts communication links 1 and 2 as the main connections from the Ground Control Station (GCS) to the Unmanned Aerial Vehicle (UAV) via a terrestrial network managed by a service provider. Alternatively, links 3 and 4 via satellite networks can serve as backups. Line of sight (LoS) operations, where GCS operators have visual contact with the UAV, primarily use link 1. Beyond visual line of sight (BLoS), operations utilise link 2 or links 3 and 4 depending on operational needs. Link 5 is shown to highlights the potential necessity for data relay channels to separate data relevant to the UAS's service from command and control messages for flight operations [12].

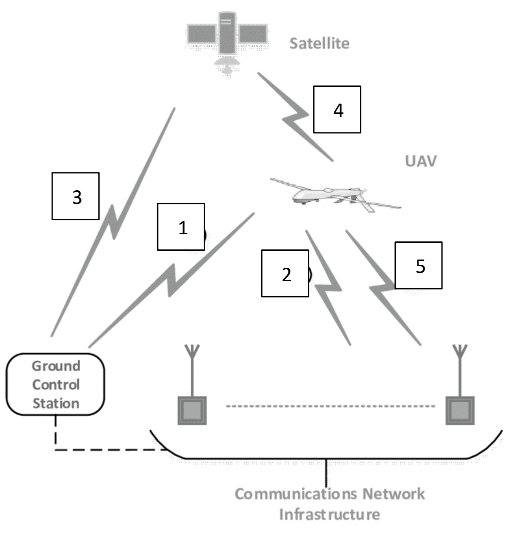

Fig. 1. UAS Architecture [12]

2.1 Modulation techniques

Effective modulation techniques are crucial for meeting the demanding requirements of UAV communication systems, ensuring reliable, high-speed, and secure data transmission across varied and dynamic operational environments. In the context of drone communication systems, the choice of modulation techniques significantly influences the robustness and security of data transmission. Commercial UAVs use spread spectrum techniques to mitigate interference from noise, jamming, and other nearby UAVs. These techniques are developed to enhance secure communications, improve resistance to jamming and detection by transmitting signals across a bandwidth wider than necessary for the data. This is achieved using a pseudo-noise (PN) code, which allows for signal despreading and data recovery at the receiver. The primary spread spectrum methods discussed are frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS) [13]. FHSS involves the pseudo-random switching of the signal across different frequencies within the bandwidth. The undisclosed algorithm adds a layer of security, making it resilient against interference, frequency jamming, and malicious interception attempts. DSSS employs pseudo-randomly generated codes to encode data at higher frequencies, enhancing resistance to interference and enabling data recovery even if certain bits are damaged during transmission. Figure 2 shows that FHSS and DSSS, two modulation techniques, applied to the carrier signal, compose Spread Spectrum modulation techniques [14].

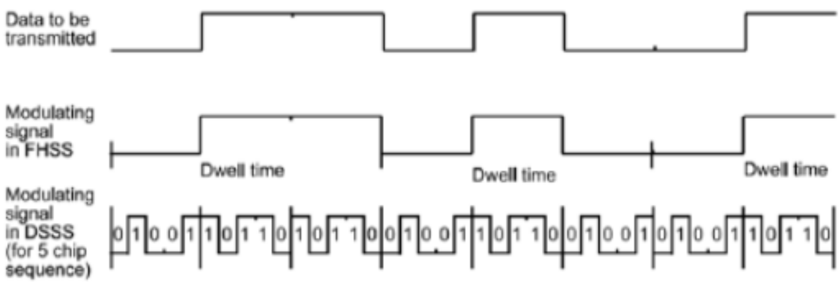

Fig. 2. Modulation technique of FHSS and DSSS [14]

Intrinsic propagation losses at specific frequencies and multipath fading pose significant challenges in UAV communications. To address these, a robust and efficient solution is needed. Orthogonal Frequency Division Multiplexing (OFDM) is well-suited for this purpose, offering high-capacity, high-speed wireless broadband multimedia networks while coexisting with current and future systems. OFDM transforms a frequency-selective channel into multiple frequency-flat subchannels. OFDM offers several advantages despite its origin in frequency division multiplexing (FDM). Subcarrier frequencies in OFDM are chosen to be mathematically orthogonal over one symbol period, achieved through digital modulation and multiplexing using an inverse fast Fourier transform (IFFT), ensuring precise generation of orthogonal signals [15]. OFDM is a digital modulation technique that divides a signal into multiple narrowband channels at different frequencies. It utilizes multiple subcarriers within the same channel, emphasizing efficient communication by mitigating interference from neighbouring signals [16]. Figure 3 shows that OFDM is an overlapping multicarrier modulation technique in which each carrier unit is created orthogonally by the gap in addition to time synchronization. These modulation techniques collectively contribute to the overall reliability, security, and performance of drone communication systems, which are crucial aspects for the success of unmanned aerial vehicles in various applications.

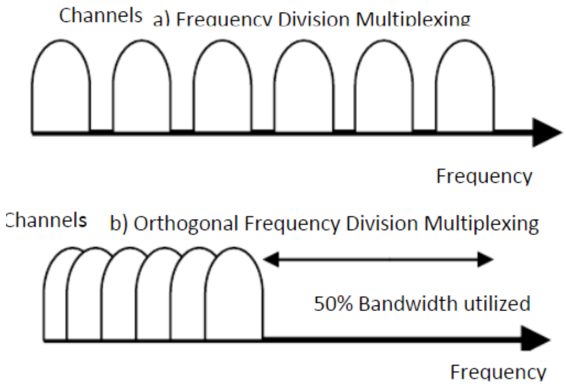

Fig. 3. OFDM Signal [17]

2.2 Transmission systems

The ongoing advancement and deployment of UAV technology across diverse applications can be accomplished by employing advanced modulation techniques and integrating them with sophisticated transmission systems. Drones rely on diverse transmission systems, each with unique features, to cater to specific communication needs. Wi-Fi, a ubiquitous technology, provides standard wireless connectivity, offering versatility and compatibility. Lightbridge, an evolved version of Da-Jiang Innovations (DJI)'s initial transmission protocol, builds upon Wi-Fi capabilities and distinguishes itself by enabling simultaneous control of both video and control signals. This advancement enhances the overall user experience, allowing for seamless operation. Ocusync, a further refinement of Lightbridge, incorporates advanced features such as Frequency Hopping Spread Spectrum (FHSS) for dynamic control and telemetry signal changes, along with Orthogonal Frequency Division Multiplexing (OFDM) encoding for robust data transmission. Notably, Ocusync is underpinned by unique software, facilitating firmware updates to introduce enhancements and optimizations, showcasing the adaptability and upgradeability of modern drone communication technologies [16]. Table 2 below summarizes the differences in transmission systems.

Table 2
Summarization of transmission systems [14, 16]

Transmission systems	Description	Benefits	Drones
Wi-Fi	Offers standard wireless connectivity that allows users to control their dedicated remote controller or a mobile device	• Cost-effective method • Portable due to the small size • Able to maintain VLOS and keep the drone at a safe distance despite the limited range	DJI Spark DJI Mavic Air DJI Mini
Lightbridge	Traditionally designed to work with their professional and enterprise level drones.	• Provides a reliable connection between the drone and the controller • Some drones using Lightbridge have customizable functions that can integrate into any industry.	DJI Phantom 4 Pro DJI Phantom 4 Advanced
Ocusync	Transmission system that has a superior transmission range to Wi-Fi and Lightbridge.	• Not as susceptible to interference • Allows multiple remote controllers to connect to the drone at one time • Offers substantial transmission ranges	DJI Phantom 4 Pro V2.0 DJI Mavic 3 DJI Mini 3 Pro

2.3 Classification of Detection Sensors

In order to effectively identify UAVs for classification purposes, understanding the classification of detection sensors is important. The detection of UAVs hinges on the meticulous selection and deployment of appropriate sensor technologies. Different types of sensors offer unique capabilities, each tailored to specific aspects of UAV detection. These sensors may include acoustic, imaging, radar, radio frequency, and hybrid which is a combination of two or more of the mentioned sensors. Each sensor possesses distinct strengths and weaknesses, making it crucial to identify and select the sensor that best fits the operational needs. By comprehending the characteristics of numerous sensors, we can strategically implement the most suited one, optimizing the detection process and enhancing our ability to classify UAVs accurately. Table 3 shows the classification of detection sensors.

Table 3
Classification of detection sensors

Sensor	Description	Pros	Cons
Acoustic [19]	Gather signals using a range of microphones, then extract and identify their acoustic features	• Enhanced reliability • Accuracy in position decoding	• Sensitive to Gaussian noise and measurement error of signal latencies. • Requires relatively high signal-to-interference radio (SIR).
Imaging [20]	Electro-optical (EO) and infrared (IR) cameras are used to identify and track UAVs	• Infrared cameras work in all weather conditions and during day or night. • They can be supported by computer-vision technologies.	• Performance is limited by weather and background temperature. • Line of sight (LoS) is necessary.
Radar [21]	Transmit electromagnetic signals which interact with the UAV	• Capable of identifying micro-Doppler signatures (MDS). • Useful for the design of an automatic target recognition (ATR) system.	• Highly limited maximum detectable range if the target has a low radar cross-section.
Radio Frequency [22]	Obtain information transmitted between UAV and its base station	• Offers the possibility to detect UAS during the pairing process of the remote control. • Grant the user additional time.	• Short reaction times. • Challenging to precisely determine Angle of Attack (AoA).
Hybrid [20]	A combination of two or more of the mentioned sensors	-	-

2.4 Jamming and Spoofing Attacks

The effective operation of UAVs hinges on sophisticated communication systems, where modulation techniques play a pivotal role and when these techniques integrated with advanced transmission systems, it facilitates the efficient functioning of various detection sensors, enabling UAVs to perform a multitude of tasks ranging from surveillance and environmental monitoring to navigation and target tracking. However, as UAVs become increasingly reliant on these intricate communication networks, they also become vulnerable to malicious activities such as jamming and spoofing attacks. UAVs often use Global Positioning System (GPS) for accurate landing, but its vulnerability to Radio Frequency (RF) interference, poses substantial threats to both civilian and military users. Jamming involves communication disruption of the target drone [20]. Adversaries in secure telecommunications are categorized as either passive or active. Passive adversaries, or eavesdroppers, intercept communications, while active adversaries, or jammers, disrupt the message or transmission medium to deny RF link communication [23]. Jamming attacks interfere with the reception of broadcast communication. Table 4 below shows the different types of jamming attacks.

Table 4
Types of jamming attacks [9, 21]

Types of Jamming Attacks	Description
Barrage	A signal with Gaussian distribution noise is sent over the communication bandwidth.
Single-tone	A high-power interfering signal is sent at the target's data exchange center frequency.
Successive-pulse	A sequence of pulses is transmitted to disrupt the communication of the target.
Protocol-aware	Involves low interference energy and low detection probability.

Misidentification between barrage and protocol-aware jamming types is common in UAVs due to their similar spectral properties. This poses a significant challenge for UAV communication systems. To address this issue, advanced machine learning techniques can be integrated into UAV signal classification algorithms. Additionally, developing specialized feature extraction methods tailored to UAV environments could enhance classification accuracy.

On the other hand, GPS spoofing occurs when an eavesdropper sends a counterfeit signal, generating a fake position or modifying the predefined one to mislead the UAV system from its intended mission [10]. A basic attack employs GPS simulation software, like software-defined radio, using a low-cost GPS signal simulator without time synchronization. Thus, GPS spoofing is feasible only when the target receiver is in signal acquisition mode. Otherwise, jamming is required for the receiver to locate other GPS signals [25]. Table 5 shows three types of spoofing attacks.

Table 5
Types of spoofing attack [8, 11]

Types of Spoofing Attacks	Description
Simple	The attacker can generate false GPS signals.
Intermediate	The attacker generates false signals while initiating the attack on each channel of the target receiver simultaneously by performing code phase alignment between real and spoofed signals.
Sophisticated	The attacker creates several signals to disrupt the frequency of other signals.

If a signal is detected as fake or spoofed, the UAV will stop taking any action and wait for new incoming signals and this verification process will continue until an authentic signal is received. The UAV employs a continuous and rigorous signal verification process to ensure it only acts on authenticated signals. This approach highlights the importance of signal authentication in UAV operations to prevent unauthorized or malicious commands from being executed. By stopping actions upon detecting a fake or spoofed signal and waiting for an authentic one, the UAV enhances its security and operational integrity, ensuring it performs tasks only under legitimate directives.

3. UAV Detection using Software-defined Radio (SDR) with Machine Learning

In this section, detection techniques using SDR are discussed utilizing radio frequency signals. Additionally, this section explores the integration of SDR with machine learning, enabling detection systems to dynamically analyze radio frequency data. This integration enhances their capability to identify and categorise signals effectively.

3.1 Software-Defined Radio (SDR)

This section introduces a variety of SDR types, offering insights derived from a range of authoritative sources. SDR is a hardware kit controlled by software that defines radio parameters and operation modes. To function fully, additional components are needed, including a single-board computer to power the radio and process data [27]. SDR contains various reconfigurable software-based components for processing and converting digital signals. Unlike traditional radio communication systems, these radio devices are highly flexible, versatile and configurable [28]. Utilizing SDR for drone detection involves intercepting and analyzing the signals transmitted between the UAV and the ground station. Typically, these signals comprise control commands transmitted from the ground station (uplink) and data transmitted from the drone (downlink) [20]. The purpose of Table 6 is to offer a systematic comprehension of the scope and detail of SDR research. By analysing these many contributions, this paper aims to extract important data about the SDR field's development and uses, enabling a more sophisticated comprehension of this research.

3.2 Machine learning algorithms

The UAV can capture multi-spectral photographs, and its operator can adjust image resolution by varying the altitude. However, interpreting high-resolution images is challenging without machine learning algorithms [29]. To identify and categorise UAVs, SDR coupled with machine learning techniques is employed. The study of machine learning involves understanding how computers acquire information without explicit programming, particularly useful when interpreting data becomes challenging [30]. Machine learning methods prove valuable tools in data mining, offering successful solutions to problems arising during analyses or when establishing relationships between various characteristics [31]. In drone identification, the support vector machine (SVM), a machine learning classifier, is utilised with sensors [32]. SDR serves as the device for radio communication systems, where a computer generates or defines transmitter modulation in wireless communication.

Table 6
Types of Software-defined Radio used for UAV detection

References	Title	SDR Type	Method	Result
Swinney *et al.*, 2022 [33]	Low-Cost Raspberry-Pi-Based UAS Detection and Classification System Using Machine Learning	BladeRF	• BladeRF SDR: 60 MBits/s, connected to a low-cost antenna (800 MHz to 6 GHz) • Raspberry Pi with GNURadio: Visualised spectrum, implemented ZMQ socket • Python script in terminal: Received data, executed	• Inference times: 15 to 28s for two-class UAS detection, 18 to 28s for classification • Raspberry Pi more suitable as a raw SDR data repeater for timely results • Two-class detection: 100% accuracy, UAS type classification: 90.9% with

			predictions with pre-trained models.	predictions ranging from 50 to 66.67%.
Tang, 2023 [16]	Drone Detection and Classification with Machine Learning	HackRF One	• Laptop with GNU Radio and HackRF One SDR: Gathers data • HackRF One, acting as a receiver, runs GNU Radio on a laptop with native Kali Linux • Custom GNU Radio block manages OFDM inputs, runs real-time predictions, and outputs results • Real-time accuracy evaluation of the model with all three drones using a fixed number of predictions.	• Models show satisfactory performance with clean OFDM data in the chamber • High signal-to-noise ratio in the rf-shielded chamber enhances precise drone detection • Outdoor models' suboptimal performance due to insufficient training data for different distances • Despite accuracy decline, models perform better at further distances • Chamber-trained model achieves 48% accuracy in 3000-sample evaluation dataset, outperforming outdoor datasets • Location and distance between drone and receiver significantly impact accuracy rate.
Eason *et al.*, 2020 [34]	Software Define Radio in Realizing the Intruding UAS Group Behavior Prediction	USRP	• UAV RF signals captured by SDR for time series data • Short-time Fourier transform (STFT) used for time-frequency spectrum • Spectrum analyses energy distribution for signal variance patterns in two UAV trajectories • Transformed matrix in time-frequency domain utilised in multiple machine learning classifiers different flying trajectories.	• Monitoring RSSI variance crucial for detecting amateur UAV presence • Sporadic RF signals valuable for detection in secure areas with evolving autonomous vehicle technology • UAVs may intermittently transmit for trajectory verification • Paper demonstrates using video signal to detect Doppler effects and RSSI variance in UAV transmission

In the realm of machine learning, diverse algorithms are applied to address specific problem sets depending on the nature of the collected data. Through the research, it has been identified key algorithms that play significant roles in this field, including K-Nearest Neighbors (kNN), linear Support Vector Classification (SVC), Random Forest (RF), and Gaussian Naive Bayes (NB). Each of these algorithms offers distinct strengths, making them valuable tools for addressing a variety of challenges in the context of machine learning. Table 7 shows the description of each algorithm of machine learning mentioned.

Table 7
Machine learning algorithms

Reference	Algorithm	Description
Xie *et al.* [8]	K-Nearest Neighbors (kNN)	In kNN, an unclassified data sample is categorised by looking at its k nearest neighbors. If the majority of these neighbors belong to a specific class, the unclassified sample is assigned to that class.
Tang [16]	Support Vector Classification (SVC)	Commonly employed for classification tasks due to its high accuracy and efficient computation. It aims to identify a hyperplane that effectively separates data points, where the hyperplane's dimension corresponds to the input features.
Aissou *et al.* [26]	Random Forest (RF)	Based on the bagging method of ensemble learning, which combines predictions from multiple decision trees using a majority voting method to improve the predictive accuracy and control over-fitting.
Ontivero-Ortega *et al.* [35]	Gaussian Naive Bayes (GNB)	A basic classification algorithm involves assigning a label based on the class with the highest posterior probability for each sample. This algorithm is ideal for quick computations, significantly faster than popular methods like Support Vector Machine (SVM) or Logistic Regression classifiers.

In conclusion, the exploration of machine learning algorithms highlights its critical roles in solving diverse problem sets tailored to the nature of the data. Each algorithm possesses unique attributes that contribute to its effectiveness in specific scenarios, underscoring the importance of algorithm selection in the success of machine learning applications. The detailed analysis provided in this research, supported by Table 7, emphasizes the nuanced capabilities of these algorithms, serving as a valuable reference for practitioners and researchers aiming to leverage machine learning techniques optimally. By understanding the strengths and appropriate applications of kNN, SVC, RF, and NB, one can make informed decisions that enhance the performance and accuracy of predictive models, ultimately advancing the field of machine learning.

4. Conclusions

This study serves as a commencement exploration into the development of UAVs detection and categorization, leveraging machine learning alongside SDR, that is cost-effective. While prior research primarily focused on visual object detection, this work shifts the focus to utilizing RF and SDRs as edge devices. This approach offers promising components for prospective UAVs detection and categorisation by harnessing capabilities like triangulation and extended detection ranges. This presents a comprehensive review focused on the classification of UAVs by integrating SDR technology with machine learning algorithms, with the ultimate goal of constructing a robust an advanced UAVs detection. The review findings reveal important implications for practical implementation such as inference times indicate that for time-sensitive applications. The observed challenges in model performance during distance evaluation underscore the need for further refinement in methodologies or the incorporation of additional data augmentation techniques to improve accuracy across different distances.

Future research should focus on imperative to expand the deployment of SDRs across a wider spectrum to enhance UAS detection capabilities. Additionally, refining real-time testing protocols to account for environmental variables is crucial for ensuring the robustness and applicability of the proposed early warning system in dynamic conditions.

Acknowledgment
The authors would like to thank all who have directly or indirectly provided assistance to support this project. This research was funded by Universiti Sains Malaysia, Short-Term Grant with Project No:304.PAERO.6315627.

References
[1] W. Shule, C. M. Almansa, J. P. Queralta, Z. Zou, and T. Westerlund, “UWB-based localization for multi-UAV systems and collaborative heterogeneous multi-robot systems,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 357–364. doi: 10.1016/j.procs.2020.07.051.
[2] O. Liebermann, J. Hansler, H. Britzky, and N. Bertrand, “Russian fighter jet forces down US drone over Black Sea,” *CNN Politics*, Mar. 15, 2023. Accessed: May 20, 2024. [Online]. Available: https://edition.cnn.com/2023/03/14/politics/us-drone-russian-jet-black-sea/index.html
[3] Delauney Guy, “Mystery drone from Ukraine war crashes in Croatia,” *BBC*, Mar. 11, 2022. Accessed: May 20, 2024. [Online]. Available: https://www.bbc.com/news/world-europe-60709952
[4] Carr Stewart, “Boeing 737 travelling at at 200mph and carrying up to 189 passengers missed drone by just 6ft in one of the closest ever near-misses in UK airspace, report reveals,” *Mail Online*, Dec. 02, 2021. Accessed: May 20, 2024. [Online]. Available: https://www.dailymail.co.uk/news/article-10268343/Boeing-737-travelling-200mph-carrying-189-passengers-missed-drone-just-6ft.html
[5] M. Pechtold, “Drone stops air traffic at Frankfurt Airport – Fraport offers high reward,” *Frankfurter Neue Presse*, Mar. 05, 2021. Accessed: May 20, 2024. [Online]. Available: https://www.fnp.de/frankfurt/flughafen-frankfurt-drohne-sichtung-verspaetungen-starts-nachtfluege-bundespolizei-gesichtet-90212643.html
[6] A. Farnworth, “Helicopter fighting Darwen Moor fire forced to land due to drone flying above incident,” *Lancshire Telegraph*, Jun. 01, 2020. Accessed: May 20, 2024. [Online]. Available: https://www.lancashiretelegraph.co.uk/news/18488435.helicopter-struggles-extinguish-darwen-moor-fire-due-person-flying-drone-incident/
[7] M. Murison, “Air Traffic Disrupted at Madrid Airport Following Drone Sighting Reports,” *dronelife*, Feb. 03, 2020. Accessed: May 20, 2024. [Online]. Available: https://dronelife.com/2020/02/03/air-traffic-disrupted-madrid-airport-drone/
[8] J. Xie *et al.*, “A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 393–430, Jan. 01, 2019. doi: 10.1109/COMST.2018.2866942.
[9] J. Pawlak *et al.*, “A Machine Learning Approach for Detecting and Classifying Jamming Attacks against OFDM-based UAVs,” in *WiseML 2021 - Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning*, 2021, pp. 61–66. doi: 10.1145/3468218.3469049.
[10] A. Shafique, A. Mehmood, and M. Elhadef, “Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models,” *IEEE Access*, vol. 9, pp. 93803–93815, 2021, doi: 10.1109/ACCESS.2021.3089847.
[11] E. Darack, “A Brief History of Unmanned Aircraft.” Accessed: Feb. 16, 2024. [Online]. Available: https://www.smithsonianmag.com/air-space-magazine/a-brief-history-of-unmanned-aircraft-174072843/
[12] C. Caicedo, “Spectrum Management Issues for the Operation of Commercial Services with UAVs,” *SSRN Electronic Journal*, Sep. 2017, doi: 10.2139/ssrn.2944132.
[13] T. J. Seebecki *et al.*, “TALLINNA TEHNIKAÜLIKOOL Infotehnoloogia teaduskond,” 2017.
[14] M. Hasan, J. M. Thakur, and P. Podder, “Design and Implementation of FHSS and DSSS for Secure Data Transmission,” *International Journal of Signal Processing Systems*, vol. 4, no. 2, 2015, doi: 10.12720/ijsps.4.2.144-149.
[15] A. R. Chadha, N. Satam, B. R. Ballal, and A. Chadha, “Orthogonal Frequency Division Multiplexing and its Applications,” 2013. [Online]. Available: https://www.researchgate.net/publication/235943582
[16] M. Tang, “DRONE DETECTION AND CLASSIFICATION WITH MACHINE LEARNING,” 2023.
[17] D. Khosla, D. Khosla Assistant Professor, E. Deptt, and S. Singh Assistant Professor, “OFDM Modulation Technique & its Applications: A Review,” 2018. [Online]. Available: www.ccsarchive.org
[18] “DJI Transmission Systems – Wi-Fi, OcuSync & Lightbridge.” Accessed: Feb. 10, 2024. [Online]. Available: https://www.heliguy.com/blogs/posts/dji-transmission-systems-wi-fi-ocusync-lightbridge#:~:text=It%20falls%20within%20the%20Lightbridge,areas%20with%20strong%20radio%20signals.
[19] X. Yue, Y. Liu, J. Wang, H. Song, and H. Cao, “Software Defined Radio and Wireless Acoustic Networking for Amateur Drone Surveillance,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 90–97, 2018, doi: 10.1109/MCOM.2018.1700423.

[20] F. L. Chiper, A. Martian, C. Vladeanu, I. Marghescu, R. Craciunescu, and O. Fratu, “Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution,” *Sensors*, vol. 22, no. 4. MDPI, Feb. 01, 2022. doi: 10.3390/s22041453.
[21] M. Ezuma, F. Erden, C. Kumar Anjinappa, O. Ozdemir, and I. Guvenc, “Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques.”
[22] S. Kunze, A. Weinberger, and R. Poeschl, “Concept for a Software Defined Radio Based System for Detection, Classification and Analysis of Radio Signals from Civilian Unmanned Aerial Systems,” in *2018 2nd URSI Atlantic Radio Science Meeting, AT-RASC 2018*, 2018. doi: 10.23919/URSI-AT-RASC.2018.8471398.
[23] A. Heuchamps, P. C. J-M Redouté Ir Greffe, P. A. Papy, and I. M. Spirlet, “Study and Design of UAS Jamming Systems.”
[24] Y. Li *et al.*, “Jamming Detection and Classification in OFDM-Based UAVs via Feature- and Spectrogram-Tailored Machine Learning,” *IEEE Access*, vol. 10, pp. 16859–16870, 2022, doi: 10.1109/ACCESS.2022.3150020.
[25] Y. H. Sung, S. J. Park, D. Y. Kim, and S. Kim, “GPS Spoofing Detection Method for Small UAVs Using 1D Convolution Neural Network,” *Sensors*, vol. 22, no. 23, Dec. 2022, doi: 10.3390/s22239412.
[26] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, “Tree-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS,” in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2021*, 2021, pp. 649–653. doi: 10.1109/UEMCON53757.2021.9666744.
[27] P. Papoci, T. Radišic, and M. Muštra, “Integration of Software Defined Radio on an Unmanned Aerial Vehicle,” in *Transportation Research Procedia*, Elsevier B.V., 2022, pp. 308–315. doi: 10.1016/j.trpro.2022.09.035.
[28] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, “A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities,” *Sensors*, vol. 22, no. 4, Feb. 2022, doi: 10.3390/s22041487.
[29] A. I. Khan and Y. Al-Mulla, “Unmanned aerial vehicle in the machine learning environment,” in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 46–53. doi: 10.1016/j.procs.2019.09.442.
[30] B. Mahesh, “Machine Learning Algorithms-A Review,” *International Journal of Science and Research*, 2018, doi: 10.21275/ART20203995.
[31] H. Tan, “Machine Learning Algorithm for Classification,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Aug. 2021. doi: 10.1088/1742-6596/1994/1/012016.
[32] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, “Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, Apr. 2018, doi: 10.1109/MCOM.2018.1700430.
[33] C. J. Swinney and J. C. Woods, “Low-Cost Raspberry-Pi-Based UAS Detection and Classification System Using Machine Learning,” *Aerospace*, vol. 9, no. 12, 2022, doi: 10.3390/aerospace9120738.
[34] J. Eason, C. Xu, and H. Song, “Software Define Radio in Realizing the Intruding UAS Group Behavior Prediction,” in *2020 IEEE 39th International Performance Computing and Communications Conference, IPCCC 2020*, 2020. doi: 10.1109/IPCCC50635.2020.9391526.
[35] M. Ontivero-Ortega, A. Lage-Castellanos, G. Valente, R. Goebel, and M. Valdes-Sosa, “Fast Gaussian Naïve Bayes for searchlight classification analysis,” *Neuroimage*, vol. 163, pp. 471–479, Dec. 2017, doi: 10.1016/j.neuroimage.2017.09.001.