IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 27, 2021, accepted June 10, 2021, date of publication June 16, 2021, date of current version July 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3089847

Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models

ARSLAN SHAFIQUE[1], ABID MEHMOOD[2], (Member, IEEE), AND MOURAD ELHADEF[2], (Member, IEEE)

[1]Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan
[2]Department of Computer Sciences, Abu Dhabi University, Abu Dhabi 59911, United Arab Emirates

Corresponding author: Arslan Shafique (arslan.shafique@riphah.edu.pk)

ABSTRACT Due to the tremendous advancement in interactive multimedia systems and technologies, security has become a major aspect. Advanced technology can be utilized for hacking autonomous systems like Unmanned Aerial vehicles (UAVs) in different ways such as spoofing and jamming. It can be spoofed by the injection of fake signals into the sensors. For the protection of the UAVs from the Global Positioning System (GPS) signal spoofing attack, we propose a new methodology by incorporating a machine learning (ML) algorithm such as Support Vector Machine (SVM). A detailed analysis of several learning algorithms is also carried out to choose the suitable learning algorithm for the proposed work. Once the suitable ML algorithm is selected, we perform K-fold analyses to develop other learning models by choosing different values of K-folds thus we called them K-learning models. The purpose of developing K-learning models is to apply voting techniques to the developed K-learning models. Moreover, the signal features used in the proposed work are jitter, jitter (absolute), jitter (local), jitter (RAP), jitter (ppq5), shimmer, shimmer (local), shimmer (dB), shimmer (apq3), shimmer (apq5) and frequency modulation. Based on these features of the signal, we train our proposed model for the detection of counterfeit GPS signals. To gauge the performance of the proposed model, we perform different experimentation analyses such as accuracy, precision, recall, and F1-score. The results and analysis show the effectiveness of the proposed work over existing techniques.

INDEX TERMS UAV, SVM, spoofing attack, signal characteristics, GPS signal.

I. INTRODUCTION

Nowadays, the autopilot systems such as UAVs or drones are frequently used for aerial surveillance systems, packet delivery, and secure communication. In a danger zone, communication signals that are exchanged between the UAVs and ground station may be lost or corrupted by incorporating possible cyber-attacks such as jamming and spoofing [1], [2]. In the case of grave danger, safe landing at the nearest safe zone or return-to-home is a challenging task. It is difficult to ensure a safe landing in unexpected zones with the weak robustness of the autopilot system against powerful cybersecurity attacks. Hence, this problem demands an intelligent decision-making system for UAVs that can take decisions on run-time to tackle and overcome the threats with less computational complexity [3]. Some of the major tasks to secure the UAVs are lightweight, small-sized and weak computational power. Due to the quite complex architecture of UAVs, it is hard to conceptualize UAVs security. However, there is a trade-off between the strong UAVs security and their expected benefits, functionalities, and cost. A detailed UAV architecture is explained by Barth *et al.* in [4].

To resists cyber-attacks, it is crucial that the UAVs' architecture must be robust. UAVs can be attacked in two ways: integrity attack and Denial of Service (DoS) attack [5]. Integrity attacks include spoofing and false data injection, while jamming, gray and black hole attack falls in the category of DoS attack.

UAV systems mostly use GPS for landing on the desired place. Although the GPS is capable of controlling the UAVS, it has been found as vulnerable to the Radio Frequency Interference [6]. Two major vulnerabilities are Jamming and GPS spoofing which can be a major threat to civilian and military GPS users. Jamming is referred to the transmission of a radio signal with a relatively higher frequency and masking the authentic signal with some noisy signal to disturb it [7]. While in GPS spoofing, an eavesdropper sends a counterfeit signal and produces a fake position or alters the pre-defined

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Saleem.

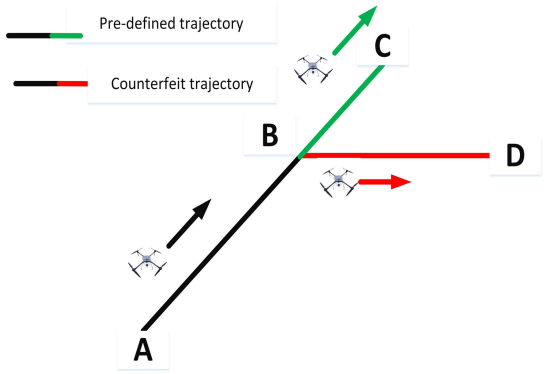

FIGURE 1. A pre-defined and a counterfeit trajectory.

position to trap the UAV system from its mission. Therefore, it is possible to spoof a military or civilian UAV by changing the trajectory from the predefined one without the user's notice. Figure 1 shows the two trajectories that will follow the UAV. The path ABC is the pre-defined trajectory, whereas the line ABD is the spoofed trajectory. If the attacker launched the spoofing attack successfully the UAV will divert from point B and will move towards point D which is not the desired location.

In recent years, security experts have found that the UAV can easily be spoofed using the GPS spoofing attack if the low-cost software and hardware are used [8]–[10]. Based on the vulnerabilities discussed in [8]–[10], GPS spoofing can be categorized into three major classes: receiver-based spoofers, GPS signal simulators, and refined receiver-based spoofers [11]. In the first category, the GPS receivers concatenate with the spoofing transmitter to find the pre-defined location. This type of spoofing is a bit difficult to detect. In the second category to spoof the GPS signal, the simulators used to send GPS signals are concatenated with the radio signals to produce a duplicate GPS signal. Combining GPS signal with the noisy signal is not needed in this method. The last category is more advanced. In this method, it is assumed that the velocity and the position of the victim receiver are precisely known. It is almost impossible to detect this type of attack using traditional-anti-spoofing attacks [12].

To resist GPS spoofing attacks, Hybrid Position Receiver (HPR) and GNSS Receiver Stand-alone (GRS) techniques are frequently used [13], [14]. The GRS techniques are based on vestigial signal defense [10] and spatial processing [15]. More details about these techniques can be found in [16]–[18]. There are also some drawbacks of HPR techniques which are explained in [19].

As the autopilot system is completely reliant on GPS location, ground station, and target. Attacks initiated by the eavesdropper are always random and opportunistic. Several components such as sensors, actuators guidance and control systems which is mounted on the UAVs, are always susceptible to a spoofing attack. In this case, an entire mission can be devastated by feeding misleading data in the form of target location or wrong trajectory for landing [20]. Using low-cost hardware or weak software installation, UAVs can easily be hacked by initiating spoofing or false data injection attack.

Spoofing attack can be of different nature which is explained below:

A. VARIOUS SPOOFING TECHNIQUES

Autopilot systems having GPS signal receivers are vulnerable to spoofing attacks. The effect of spoofing attack may depend on the robustness of the system i.e., the more the robust system, the more the resources at the attacker's end will be required to expose the system.

- **Simple spoofing**
  In simple spoofing, attackers can generate false Global GNSS signals. it can be used in practice by low-cost hardware and software [21].
- **Intermediate spoofing**
  In this scenario, the attacker generates false signals, while, initiating the attack on each channel of the target receiver simultaneously by performing code phase alignment between genuine and spoofed incoming signals [22].
- **Spoofing with multiple antennas**
  It is an advanced technique mainly used against several antenna receivers, in which the attacker generates multiple signals to disturb the frequency of the other signals [23].
  To protect the UAVs from GPS spoofing attacks, in this paper, an ML model is proposed which is based on the SVM and voting techniques such as hard and soft voting. The proposed system for the detection of spoofed GPS signals is activated whenever a GPS signal is received by the UAV. The UAV will not perform any action until it receives the GPS signal which is sent by the authentic user. If a counterfeit GPS signal is received by the UAV, it will wait for the next signal until it receives the authentic signal. The classification of the counterfeit and an original GPS signal will be based on the features which are explained in section III. Once the authentic GPS signal is received, the UAV will act accordingly. The main advantages of the proposed model are computationally efficient and can easily be implemented for real-time applications.

B. CONTRIBUTIONS OF THE WORK

The major contributions of this paper are as follows:

- We have proposed a security system that detects the authenticity of the GPS signal; whether the signal is spoofed or authentic. The proposed system is incorporated with ML algorithms that help to classify the two categories of the signal.
- Different characteristics of signals are incorporated as features that are used to classify the spoofed and authentic signals.
- Several machine learning algorithms are investigated to select the most appropriate learning algorithm for the

proposed work. The reason being is some of the ML algorithms such as logistic regression and SVM having a sigmoid kernel do not provide better results.
- Different learning models using K-fold analyses are also created by selecting different values of K-folds. To further enhance the accuracy of the proposed model, voting techniques are integrated to choose a learning model which classifies the signal with the highest accuracy shown by a specific learning model among the other proposed learning models.
- Different experimentation analyses such as accuracy, precision, recall and F1-score are performed to evaluate the effectiveness of the proposed work.

C. MOTIVATIONS

UAVs are useful and resourceful in surveillance and intelligence operations [24]. The deployment of UAV security systems demands tremendous material investment, time and a great amount of mind. In the last few years, several security protocols are proposed to protect the UAVs from signal spoofing attacks [25]–[29]. Some of them are vulnerable to jamming and spoofing attacks [19], [30].

As the vulnerable UAV system is composed of such components which are not robust can be easily hijacked by deploying cyber-attacks [31]. To make the UAV system robust, it should be capable of resisting cyber-attacks such as WiFi attacks, DoS attacks and signal spoofing attacks. To hijack the UAVs and disconnecting the communication systems, signal spoofing attacks are at the top priority of the attackers. Signal spoofing attacks can be performed in different ways; a) sending higher frequency signals, (b) false data injection and (c) high gain antenna spoofing [32], Due to the different spoofing attack strategies, the UAVs can be risky to execute several operations such as search and rescue operation, packet delivery and disaster management. This is the basic motivation behind this research work Therefore, to protect the UAVs from signal spoofing attacks, there must be an intelligent signal spoofing detection protocol that can classify the authentic and spoofed signals efficiently.

II. LITERATURE REVIEW

GPS signal spoofing is an act of producing counterfeit signals to take control and hijack UAVs. To reduce the signal spoofing threats, there has been growing interest to develop such intrusion detection systems that can detect GPS signal spoofing with maximum accuracy. Signal spoofing techniques can be categorized as (1) signal processing techniques, that helps to collect the raw data from signals and process them accordingly, (2) hardware techniques, which need multiple sensor and control systems and (3) a combination of hardware and signal processing techniques, that collects the raw signals data and process them using the control systems and signal processors.

In the past few years, there has been a variety of work has been proposed to detect the spoofed signals. For instance, receiver autonomous integrity monitoring (RAIM) is the most frequently used technique to detect signal spoofing attacks [33]. Signal spoofing attacks can be controlled using intrusion detection systems, such as anti-spoofing mechanisms [34]–[36]. In [37], sedjelmaci *et al.* proposed a rule-based IDS to differentiate between the spoofed and authentic signals. Also, the proposed system is useful to detect jamming and false information insertion detection attacks. To achieve the desired purpose, several rules are defined based on the fixed threshold values. However, fixed threshold value techniques may misclassify the correct predictions. In [38], a new IDS is designed that incorporates behavior rule specifications. As the system used only a few behavior indicators, the system is weak and fails to withstand cyber-attacks on UAVs. In [39], Muniraj *et al.* proposed a mitigation mechanism for UAVs against cyber-attacks such as actuator-based attacks. In this work, only actuator-based attacks are handled to protect the UAVs from hijacking. In [40], Xiao *et al.* presented a user-centric IDS for UAVs that incorporates reinforcement learning for attack detection. From the existing work present above, we can analyze that the traditional IDSs have major limitations.

In this paper, we have used different ML algorithms to proposed such a mechanism that can detect authentic and spoofed signals. For the time-efficient attack detection system, the advent of ML-based IDS has made it possible to detect cyber-attacks in UAVs with significant accuracy. Moreover, the use of deep learning techniques also arises issues with big data collection. However, some of the ML algorithms do not perform better on the specific data set. The performance of several ML algorithms may vary with the nature of the data. Therefore, we also propose the analysis of the performance of the different ML algorithms to select a suitable ML algorithm for the proposed model.

The rest of the paper is organized as follows: In section III, a brief overview of the SVM is given. While section IV provides the proposed work for the detection of spoofing attacks. Moreover, K-fold analysis is also presented in this section. Section V is devoted to the analysis of the proposed work and section VI concludes the proposed work.

III. SUPPORT VECTOR MACHINE

SVM is a classifier that classifies future predictions into different classes [41]. As the SVM is a supervised learning algorithm, there must be a portion of the dataset for training purposes. In the proposed work, SVM is implemented to classify the GPS signals into two categories; whether it belongs to the spoofed family or authentic.

To accomplish the classification task, several inputs/feature vectors are required. The number of features used in the dataset represents the dimensions of the dataset. For instance, if the dataset contains ten features, the data would be ten-dimensional. It can be represented as:

$$\text{For N-D dataset: } Y = X_1, X_2, X_3, X_4, \ldots . X_N$$

where $X_1, X_2, X_3, \ldots . X_N$ are the independent features on the basis which SVM predicts the feature event (Y).

While preparing the dataset, the number of features and the number of output labels do not need to be equal. Instead, it may vary depending upon the required number of output classes. To classify the data points into their respective class, SVM uses a line or a hyperplane. For a 2-Dimensional dataset, a line (support vector) is used to classify the data with maximum margins. Whereas, in the case of higher dimensions, a hyperplane is used which can be express as:

$$Cx + w = 0 \tag{1}$$

where w is the bias and C is a vector of the same dimension as the input feature vector x. As we used a 7-dimensional dataset in the proposed work, Cx can be represented as:

$$C^1 * x^1 + C^2 * x^2 + C^3 * x^3 + C^4 * x^4 + C^5 * x^5 + C^6 * x^6 + C^7 * x^7$$

While making predictions, following expression can be incorporated:

$$Y = sign(Cx + w) \tag{2}$$

where *sign* is dependent on the input, it returns $+1$ and -1 if the inputs are positive or negative respectively. x_i is feature vector and y_i is the label that can be $+1$ or -1. It can be written as:

$$\begin{cases} Cx - w \geq +1 & y_i = +1 \\ Cx - w \leq -1 & y_i = -1 \end{cases} \tag{3}$$

SVM also uses different kernels for classification purposes. The kernel can be polynomial, rbf, linear or sigmoid [42]. We have used all these kernels in the implementation of SVM for the proposed work and reported the results in section V.

IV. PROPOSED GPS-SPOOFING DETECTION MECHANISM

For the protection of UAVs from hijacking, UAVs must have such a mechanism that can detect spoofed signals not only with perfection, it should also be time-efficient. To accomplish the desired tasks, it is not the right choice to use auxiliary equipment. It can increase the cost as well the load of the UAVs. UAVs are normally equipped with Inertial Measurement Units (IMU) sensors, control systems, and camera sensors. Incorporating IMU to detect spoofing attacks is a relatively simple and low cost, but it has a cumulative error in gauging velocity [43]. That is the reason, we develop such a methodology that can detect spoofing with a minimum error rate. Figure 2 shows the generalized flow diagram of the proposed work.

As the UAVs receive so many signals at a time, but the questions arise here that how the UAV will extract the GPS signal from all those signals. Most of the signals have a single frequency i.e Radio signals transmit with a single specific frequency like 1KHz or 3KHz and so on. However, GPS signal has some specific characteristics that make it different from other signals [44]. Transmitting simultaneously navigation data using binary phase-shift keying (BPSK) and several ranging codes are included in the characteristic of

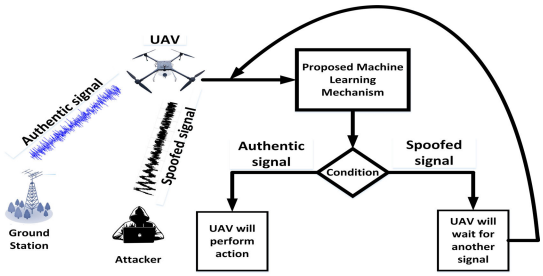

FIGURE 2. Generalized flow diagram of the proposed work.

GPS signals. Moreover, most of the civilian or military GPS devices using two different GPS frequencies at a time [45].

To detect the GPS counterfeit and authentic signal spoofing, an ML-based security system is proposed. The main purpose of the purpose work is to classify the spoofed and original GPS signal. UAVs are mostly controlled by GPS signals. It is important to receive the right destination location by the UAVs in order to land safely at the desired place. The major threat for the UAV is the spoofing attack. To resist this type of attack, we propose an ML model in which SVM and voting techniques are incorporated. To achieve the desired task, the proposed model is divided into two sections: (a) preparation of a new ML model based on one specific ML algorithm such as SVM and (b) generation of a different learning model by selecting the appropriate values of K in K-fold analysis. In the first section of the proposed model, a dataset is taken as an input that is used for both training and testing purposes. The features used in the dataset are the signal characteristics. A training phase comes first followed by the testing phase. Once the model is trained, an unknown signal is given as an input to test the proposed model. At this stage, an initial model is prepared. The same procedure is repeated to test several ML models and select a model in which the highest accuracy is archived. To further improve the accuracy of the proposed model, five more learning models are prepared by selecting the different values of K using K-fold analysis. In the last, voting techniques such as hard and voting are applied to select the final learning model by which the signal is classified.

The proposed scheme has several advantages. First, it effectively uses the sensors to detect the signals, therefore we do not need to add auxiliary equipment in UAV. Second, the proposed scheme is lightweight and can easily be implanted in real-time applications. Third, depending on the efficiency of sensors to detect the signals, it can resist the signal spoofing attacks. The flow diagram for the proposed scheme is shown in Figure 3. The detail of the proposed methodology is described given below:

To develop a GPS signal spoofing attack detection technique, the following steps are under consideration:

- Take a dataset that consists of different characteristics of GPS signal such as jitter, jitter (absolute), jitter (local), jitter (RAP), jitter (ppq5), shimmer, shimmer(local), shimmer(dB), shimmer(apq3) and shimmer (apq5).

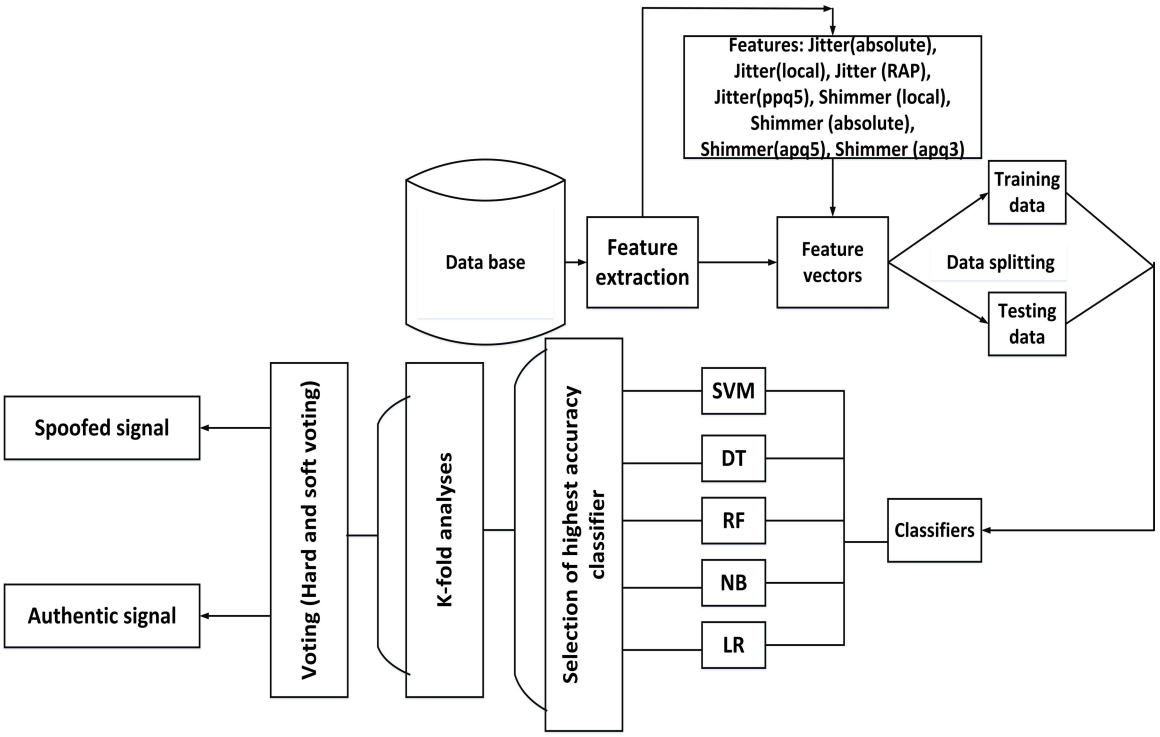

FIGURE 3. Flow diagram of the proposed work.

- To classify the signal, whether it is genuine or spoofed, first, it is required to extract the features from the received signal. The explanation of features used in the proposed scheme is given below:

A. SIGNAL CHARACTERISTICS AS FEATURES

In the proposed work, we have used signal attributes such as ''jitter'', ''Shimmer'' and their subcategories as features. Based on the numeric values of the features, our algorithm detects whether the signal is spoofed or authentic. When the UAV receives any signal, the proposed model will extract the feature values from the received signal and make a feature vector ie. $F_{vec} = f_1, f_2, f_3, f_4, \ldots . f_n$. The values in the feature vector will be compared with each feature vector in the data set using the proposed model. After applying the proposed model, if it declares the signal is sent from the authentic user, the UAV will be ready to take action accordingly.

On the other side, if the signal will declare fake or spoofed, the UAV will decline to take further action and wait for other incoming signals. This process of receiving the signal will continue until the UAV will have an authentic signal. Once the UAV will have an authentic signal, it will act accordingly and after the completion of the task, the same process will repeat for another signal.

To classify the signal, jitter and Shimmer are used as the features. The other features of signal such as frequency, mean, root mean square, and range are used in the related works [46]–[48]. According to existing work, [46]–[48], while using features other than jitter and shimmer, the overall accuracy of the model is not good enough to classify the signal correctly. Moreover, there are ten parameters are used as features because only two or three parameters are not suitable to classify the signal correctly. Therefore, to achieve the high accuracy of the model, we have used ten parameters as features which are explained below:

1) **Jitter**
   Jitter refers to how much difference between the two periods. It can be expressed by four parameters: the absolute jitter (jitta), the local (jitt), the five points period perturbation Quotient (ppq5) and the relative average perturbation (rap). The jitta is represented in μs and the other three terms can be represented in percentage [49]–[51].
2) **Jitter (absolute)**
   It is referred to the absolute difference between the two consecutive periods of the signal. It is also known as jitta. Mathematically it can be calculated as:

$$jitta = \frac{1}{M-1} \sum_{j=1}^{M-1} (|T_j - T_{j-1}|) \tag{4}$$

   where T_j is the duration in seconds of each period and 'M' is the total number of periods. Table 1 shows the intervals for jitta in which the proposed

TABLE 1. Defined intervals for jitta.

[01.00	25.50]	⇒ for original signal
[25.75	75.55]	⇒ for spoofed signal
[75.50	100.0]	⇒ for original signal

model will check whether the signal is spoofed or original.

3) **Jitter (local)**
It is the average absolute period of three consecutive periods, divided by the total average period of the signals. It is also called jitt. Mathematically it can be cal written as:

$$jitt = \frac{\frac{1}{M-1}\sum_{j=1}^{M-1}(|T_j - T_{j-1}|)}{\frac{1}{M} - \sum_{j=-1}^{M}(T_j)} \quad (5)$$

The jitter(local) intervals for the original and spoofed signal is defined in Table 2:

TABLE 2. Defined intervals for jitter(local).

[01.00	25.50]	⇒ for original signal
[25.75	75.50]	⇒ for spoofed signal
[75.75	100.0]	⇒ for original signal

4) **Jitter (RAP)**
It represents the average absolute difference of a single period and the average of that period with its two nearby periods, divided by the total average period of the signals. Jitter (rap) can be expressed as:

$$RAP = \frac{\frac{1}{M-1}\sum_{j=1}^{M-1}(|T_j - (\frac{1}{3}\sum_{m=j-1}^{j+1}(T_m))|}{\frac{1}{M} - \sum_{j=-1}^{M}(T_j)} \quad (6)$$

The jitter (RAP) intervals for the original and spoofed signal is defined in Table 3:

TABLE 3. Defined intervals for jitter (RAP).

[100.0	75.50]	⇒ for original signal
[75.00	25.50]	⇒ for spoofed signal
[25.25	01.00]	⇒ for original signal

5) **Jitter (ppq5)**
It represents the average absolute difference of a single period and the average of that period with its four nearby periods, divided by the total average period of the signals. It can be represented in percentage which can be calculated as:

$$RAP = \frac{\frac{1}{M-1}\sum_{j=1}^{M-1}(|T_j - (\frac{1}{5}\sum_{m=j-2}^{j+2}(T_m))|}{\frac{1}{M} - \sum_{j=-1}^{M}(T_j)} \quad (7)$$

The jitter (ppq5) intervals for the original and spoofed signal is defined in Table 4:

TABLE 4. Defined intervals for jitter (ppq5).

[01.00	25.50]	⇒ for original signal
[25.75	75.50]	⇒ for spoofed signal
[75.50	100.0]	⇒ for original signal

6) **Shimmer**
The methodology to calculate the shimmer is similar to the jitter. The only difference between the jitter and shimmer is that the jitter refers to the periods of the signal while the shimmer considers the maximum peak amplitude of the signal. For shimmer, there are also four related terms such as shimmer(local) in the percentage of the average amplitude, shimmer(absolute) in dB (Shdb), the three-point Amplitude Perturbation Quotient (apq3), and the five-point Amplitude Perturbation Quotient (apq5) both are also in percentage.

7) **Shimmer (local)**
Shimmer represents the average absolute difference between any two consecutive amplitudes, divided by the total average amplitude of the signals. It is also called shim. Mathematically, it can be represented as:

$$Shim = \frac{\frac{1}{M-1}\sum_{j=1}^{M-1}(|A_j - A_{j+1}|)}{\frac{1}{M} - \sum_{j=1}^{M}(A_j)} \times 100 \quad (8)$$

The shimmer(local) intervals for the original and spoofed signal is defined in Table 5:

TABLE 5. Defined intervals for shimmer (local).

[100.0	75.50]	⇒ for original signal
[75.00	25.50]	⇒ for spoofed signal
[25.55	01.00]	⇒ for original signal

8) **Shimmer(db)**
It is the average absolute logarithmic between any two consecutive amplitudes and it is also called ShdB and is given in *dB*. It can be calculated as:

$$Shdb = \frac{1}{M-1}\sum_{j=1}^{M-1}(|20 * log(\frac{A_{j=+1}}{A_j})|) \quad (9)$$

The Shdb intervals for the original and spoofed signal are defined in Table 6:

TABLE 6. Defined intervals for shimmer (db).

[00.50	24.75]	⇒ for original signal
[25.00	74.75]	⇒ for spoofed signal
[75.00	99.50]	⇒ for original signal

9) **Shimmer (apq3)**
It is the average absolute difference between the amplitude of any one period and the mean of its two nearby periods amplitudes (nearby period amplitudes can either be one previous and the other is

subsequent or it can be two consecutive), divided by the average of the total amplitude of the signal. The expression for the calculation of shimmer (apq3) is given as:

$$apq3 = \frac{\frac{1}{M-1}\sum_{j=1}^{M-1}(|A_j - (\frac{1}{3}\sum_{m=j-1}^{j+1}(A_m))|}{\frac{1}{M} - \sum_{j=1}^{M}(A_j)} \tag{10}$$

The shimmer(apq3) intervals for the original and spoofed signal is defined in Table 7:

TABLE 7. Defined intervals for shimmer (apq3).

[100.0	75.50]	⇒ for original signal
[75.00	25.50]	⇒ for spoofed signal
[25.25	01.00]	⇒ for original signal

10) **Shimmer (apq5)**

Shimmer(apq5) is identical to the shimmer(apq3), the only difference is that shimmer(apq5) takes 4 neighbor periods amplitude instead of two. It can be calculated as:

$$apq5 = \frac{\frac{1}{M-1}\sum_{j=2}^{M-2}(|A_j - (\frac{1}{5}\sum_{m=j-2}^{j+2}(A_m))|}{\frac{1}{M} - \sum_{j=1}^{M}(A_j)} \tag{11}$$

The shimmer(apq5) intervals for the original and spoofed signal is defined in Table 8:

TABLE 8. Defined intervals for shimmer (apq5).

[01.00	25.50]	⇒ for original signal
[25.75	75.25]	⇒ for spoofed signal
[75.5	100]	⇒ for original signal

11) **Frequency modulation**

Modulation is a technique of mixing an original signal with a high-frequency signal or a carrier signal. Although the GPS signal will have a high frequency, due to security measures, before sending the GPS signal, it will be modulated with a specific frequency. i.e 250 MHz to 300 MHz. The demodulator which is mounted on the UAV will demodulate the signal. If the extracted signal does not lie in the selected frequency range, our model will declare the GPS signal as a spoofed signal and the UAV will not perform any action.

The attacker can send the GPS signal in two ways (a) GPS signal with modulation (b) GPS signal without modulation. The attacker doesn't know the frequency of the carrier signal by which the original GPS signal is modulated. In this case, the carrier signal will also act as a secret key signal which must be kept confidential as a result, the security of the system will further enhance.

The dataset that we created is according to the intervals explained above. It is used to classify the signals into two categories: 1) spoofed signal 2) authentic signal. Once the dataset is created, it will be divided into two sections, one is for training purposes, while the remaining part of the data will be used for testing purposes. The splitting of the data is performed randomly. A random portion of the data is selected for training and testing purpose. We have applied different ML algorithms on our proposed dataset such as linear regression, Naïve Bayes, decision tree, SVM with different kernels (sigmoid, polynomial, Gaussian, and nonlinear), and random forest. After applying such algorithms, we have analyzed that some of them such as linear regression SVM (with the sigmoid kernel) do not perform well on the proposed dataset which we have created. The detailed analyses are given in section V.

To gauge the accuracy of the proposed model on a different portion of the dataset, we have performed a K-fold analysis.

B. K-FOLD ANALYSIS

We evaluate the performance of the model by selecting a specific percentage for the test samples randomly. Therefore, when we evaluate the proposed model multiple times by selecting the random portion of the dataset for testing and training purposes, the proposed model shows significantly different accuracy values every time. This happens because, in every iteration, the test and training data change. Therefore, it is not suggestible to test the proposed model only a single time for evaluation. On the other side, different ML algorithms show different accuracy values for the proposed model. For the selection of the best learning algorithm for the proposed work, we have performed K-fold experimentation. The main aim behind K-fold experimentation is that each sample in the dataset has the opportunity of being tested. The number of iterations to evaluate the performance of the proposed work using K-fold cross-validation depends on the value K. For instance, a dataset containing samples; let's say fifty samples, and anyone wants to test the model by selecting each sample as a test sample in every iteration, the value of K should be fifty or we can say that the value of k must be equal to the total number of samples (N) present in the dataset ($K = N$). For each iteration, the equation will be:

$$\begin{cases} \text{if Testing sample} & \text{T} = 1 \\ \text{Training sample} & \text{K} - 1 \end{cases} \tag{12}$$

In the proposed work, we have tested the model in two ways cross-validation methods. We called it two ways because, for the first time, we have split the dataset into 'N' parts. However, testing each sample in the big data will lead to high computational complexity. Therefore, instead of splitting the data into 'N' parts, we have chosen different values of K, (i.e. K = 5, K = 10, K = 15, K = 20). For K = 10 means that we have performed

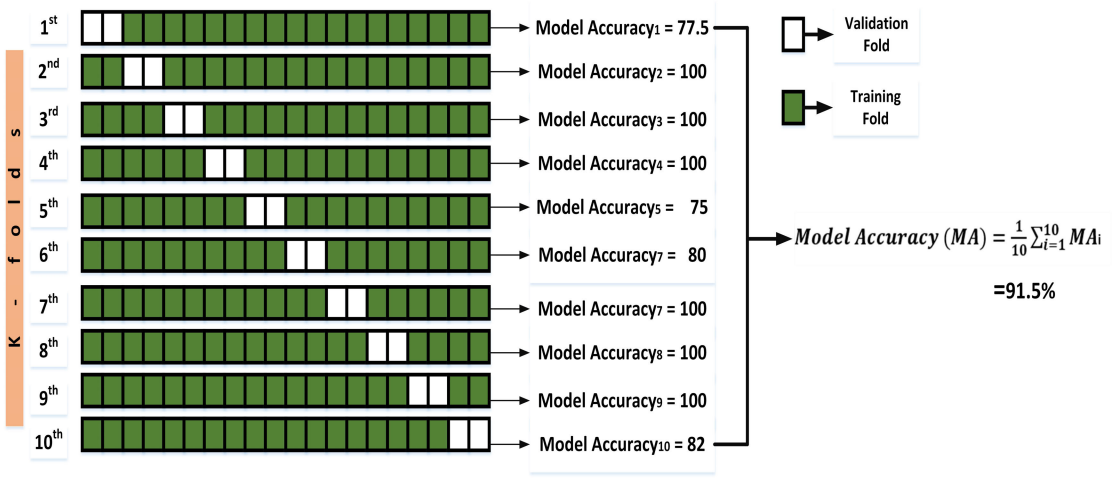

FIGURE 4. K-fold experimentation: when ten percent of the dataset is chosen in each iteration as a training fold.

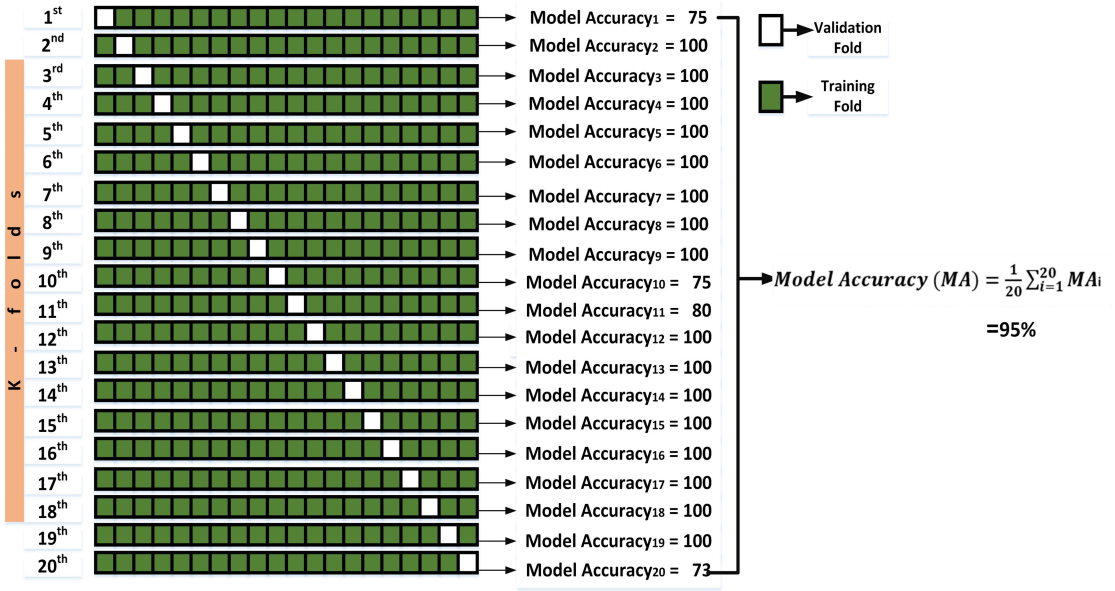

FIGURE 5. K-fold experimentation: when five percent of the dataset is chosen in each iteration as a training fold.

10 iterations to evaluate the performance of the proposed model. While for the other values of K, the number of iterations will be accordingly. Figures 4 and 5 shows 'k = 10' and 'k = 20' iteration validation processes, respectively.

- After performing the K-fold analysis on the proposed dataset, we have trained our proposed model for the prediction of the nature of the signal (spoofed or authentic).
- Finally, to evaluate the performance of the proposed work, we will calculate its accuracy, precision, recall, and F1 score. Table V gives the statistics and the comparison of the proposed work with the existing ones.

C. VOTING TECHNIQUES

After performing the K-fold analysis on the proposed model which is developed by incorporating the SVM, we have created five more different models (M_1, M_2, M_3, M_4, M_5) to develop a voting classifier. For the classification purpose, two voting techniques are considered; (a) hard voting (b) soft voting.

1) HARD VOTING

In hard voting, the voting classifier counts the number of votes and then assigns a particular class to the test sample. In case of the proposed work, we have built the first four models using cross-validation in which the values of K are $K = 5$, $K = 10$, $K = 15$ and $K = 20$. These four models have given the name K-learning models, While the fifth model is built by selecting the random training data (75%) from the whole dataset. The accuracy score for the K-learning models is mentioned in Figure 6 where it can be seen that the votes for the class A is more than the class B.

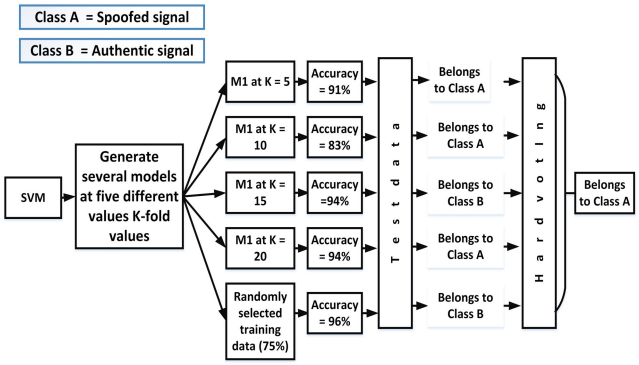

FIGURE 6. Assigning a particular class by incorporating hard voting.

Therefore, the voting classifier declared that the test sample belongs to the class B,

2) SOFT VOTING

In soft voting, rather than counting the votes, the probability of occurring the events $P(CA)$ and $P(CB)$ is considered. A test sample is tested through each K-learning model and calculates the probability occurrence. In Figure 7, the probability occurrence of a test sample corresponding to each model is shown.

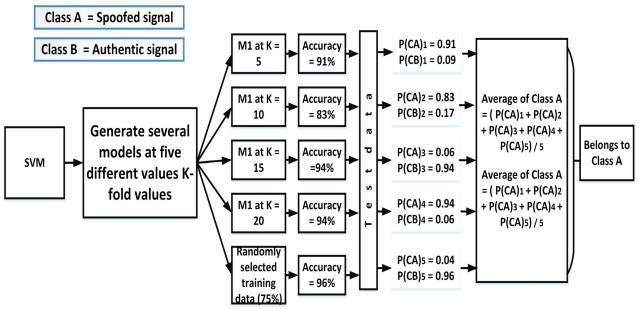

FIGURE 7. Assigning a particular class by incorporating soft voting.

Once all the probabilities are calculated, the voting classifier takes an average and then assigns a specific class to a test sample as given below:

$$\text{Probability of class A} = \frac{P(CA)_1 + P(CA)_2 + \ldots + P(CA)_5}{5} \tag{13}$$

$$\text{Probability of class A} = \frac{0.91 + 0.83 + 0.06 + 0.94 + 0.04}{5} = 55.6$$

$$\text{Probability of class B} = \frac{P(CB)_1 + P(CB)_2 + \ldots + P(CB)_5)}{5}$$

$$\text{Probability of class A} = \frac{0.09 + 0.17 + 0.94 + 0.06 + 0.96}{5} = 44.4 \tag{14}$$

V. PERFORMANCE EVALUATION FOR THE PROPOSED MODEL

The proposed work is implemented on python 3.7. For this, we have used the Jupyter notebook. Moreover, the specifications of the system on which the proposed model is tested are 8GB RAM, Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz. To gauge the performance of the proposed model, a number of statistical analyses are performed which are outlined below:

A. CONFUSION MATRIX

A confusion matrix is a two-dimensional array that is useful to calculate the parameters (precision, accuracy, and recall) that reveals the model's performance. The confusion matrix generated by incorporating SVM with polynomial kernel for the proposed work is displayed in Table 9.

TABLE 9. SVM (polynomial-kernel) confusion matrix for the proposed model.

Total No. of Test Samples (N)	Predicted Authentic Signal	Predicted Spoofed Signal
Actual Authentic Signal	38 (True positive(TP))	1 (False Negative(FN))
Actual Spoofed Signal	0 (False positive(FP))	41 (True Negative(TN))

The confusion matrices corresponding to the different ML algorithms for the proposed model are given in Table 10:

B. CLASSIFICATION ACCURACY

Accuracy reveals that how many true predictions are made by the model. More the true prediction will result in high accuracy.

$$\text{True predictions} \propto \text{accuracy}$$

It can be calculated as:

$$\text{Accuracy} = \frac{\text{Correctly predicted events}}{\text{total number of samples}} \tag{15}$$

OR

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{16}$$

According to Table 9, the accuracy of the proposed model will be:

$$\text{Percentage accuracy} = \frac{38 + 41}{38 + 1 + 0 + 41} = 98.7\%$$

C. PRECISION

It is the ratio of the true positive observations and the total number of true and false positive observations. It can be express as:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

According to the values given in Table 9, the precision of the proposed model is:

$$\text{Precision} = \frac{38}{38 + 0} = 1$$

TABLE 10. Confusion matrices generated using several ML algorithms for the proposed model.

Total No. of Test Samples (N)	Predicted Authentic Signal	Predicted Spoofed Signal
	Linear Regression	
Actual Authentic Signal	5	38
Actual Spoofed Signal	0	37
	Naive Bayes	
Actual Authentic Signal	43	0
Actual Spoofed Signal	6	31
	SVM (Sigmoid)	
Actual Authentic Signal	2	41
Actual Spoofed Signal	26	11
	SVM (Linear)	
Actual Authentic Signal	37	0
Actual Spoofed Signal	37	0
	SVM (rbf)	
Actual Authentic Signal	43	0
Actual Spoofed Signal	1	36
	SVM (polynomial)	
Actual Authentic Signal	38	1
Actual Spoofed Signal	0	41
	Decision Tree	
Actual Authentic Signal	43	2
Actual Spoofed Signal	0	35
	Random Forest	
Actual Authentic Signal	43	2
Actual Spoofed Signal	0	35

D. RECALL

It defines the sensitivity of the model. To make the model ideal in terms of recall, FN should be zero. As FN increases, the denominator will also increase which results in a decrease in the overall value of recall, which is not required for any ML model. Recall can be calculated as:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{17}$$

For the proposed model, recall value according Table 9 will be:

$$\text{Recall} = \frac{38}{38 + 1} = 0.97$$

E. F1-SCORE

F1 score is dependent on both precision and recall. It will be maximum if both the precision and the recall values are equal to 1. Mathematically, it can be calculated as:

$$F1 = 2 \times \frac{precision \times recall}{precision + recall} \tag{18}$$

TABLE 11. Analysis of proposed work corresponding to the different ML algorithms.

ML algorithms schemes	Kernels	Accuracy (%)	Precision lation	Recall geneity	F-score
Linear Regression		54.00	1.000	0.116	0.208
Naive Bayes		94.00	0.877	1.0008	0.934
SVM	Sigmoid	18.00	0.0714	0.046	0.056
	Linear	47.50	0.462	1.000	0.632
	rbf	98.75	0.997	1.000	0.988
	Polynomial	100	1.000	1.000	1.000
Decision Tree		98.75	1.000	0.977	0.988
Random Forest		98.5	1.000	0.9556	0.9773

TABLE 12. Accuracy Analysis (%).

K-folds	LR	DT	RF	NB	SVM (sigmoid Kernel)	SVM (linear Kernel)	SVM (rbf Kernel)	SVM (polynomial Kernel)
K = 5	51.5	85.5	86.5	80.5	22.5	56.5	85.5	92.5
K = 10	51.5	93.5	93.5	89.5	13.5	51.5	91.5	92.5
K = 15	51.5	95.5	96.5	90.5	13.5	51.5	95.5	96.5
K = 20	51.5	96.5	97.5	91.5	13.5	51.5	96.5	96.5
Average	51.5	92.5	93.5	88.5	15.5	52.5	92.5	94.5

TABLE 13. Precision Analysis (%).

K-folds	LR	DT	RF	NB	SVM (sigmoid Kernel)	SVM (linear Kernel)	SVM (rbf Kernel)	SVM (polynomial Kernel)
K = 5	0.34	0.83	0.83	1.00	0.31	0.34	1.00	1.00
K = 10	0.32	0.91	0.92	1.00	0.32	0.32	1.00	1.00
K = 15	0.33	0.94	0.95	0.9	0.32	0.34	0.99	0.99
K = 20	0.33	0.96	0.96	1.00	0.33	0.33	1.00	1.00
Average	0.33	0.91	0.95	0.99	0.32	0.33	0.99	0.99

TABLE 14. Recall analysis.

K-folds	LR	DT	RF	NB	SVM (sigmoid Kernel)	SVM (linear Kernel)	SVM (rbf Kernel)	SVM (polynomial Kernel)
K = 5	0.50	0.90	0.90	0.78	0.15	1.00	0.90	0.91
K = 10	1.00	0.80	0.80	0.60	0.32	1.00	0.79	0.92
K = 15	1.00	0.93	0.93	0.79	0.15	1.00	0.92	0.93
K = 20	1.00	0.95	0.95	0.81	0.14	1.00	0.93	90.95
Average	1.00	0.89	0.89	0.74	0.19	1.00	0.88	0.92

TABLE 15. F1 score analysis.

K-folds	LR	DT	RF	NB	SVM (sigmoid Kernel)	SVM (linear Kernel)	SVM (rbf Kernel)	SVM (polynomial Kernel)
K = 5	0.50	0.81	0.81	0.75	0.31	0.50	0.88	0.95
K = 10	0.48	0.90	0.90	0.87	0.20	0.48	0.94	0.95
K = 15	0.49	0.93	0.93	0.89	0.20	0.50	0.95	0.95
K = 20	0.49	0.95	0.95	0.89	0.19	0.49	0.96	0.97
Average	0.49	89.75	89.75	85.00	22.50	49.00	95.00	95.50

TABLE 16. Comparison of the proposed work with the existing ones.

ML algorithms schemes	Accuracy (%)	Precision lation	Recall geneity	F-score
Proposed	99.00	0.98	0.99	0.98
Ref [52]	97.80	0.97	0.96	0.96
Ref [53]	96.60	0.96	0.98	0.96
Ref [54]	88.91	0.90	0.92	0.90
Ref [55]	87.21	0.88	0.90	0.86
Ref [56]	85.38	0.81	0.88	0.0.89

According to Table 9, F1 score for the proposed model will be:

$$\text{F1} = 2 \times \frac{1 \times 0.97}{1 + 0.97} = 0.98$$

The scores of the different metrics when incorporating decision tree, SVM, LR, RF, and NB for the proposed model are given in Table 11. Based on the analysis, we have selected SVM (with the polynomial kernel) for the proposed work, because it gives better results as compared to the other ML algorithms as can be seen in Table 11. Once the suitable ML algorithm is selected for the proposed work, we have developed four different models (K-learning models) using the K-fold validation method. The statistical results for the K-learning models are given in Tables 12, 13, 14 and 15.

Moreover, we have also made a comparison between the proposed work with the existing work as given in Table 16. From Table 16, it can be clearly visualized that the proposed model exhibits better results than the existing ones in terms of accuracy, precision, recall, and F1 score.

VI. CONCLUSION

In this paper, a new ML model is proposed to classify the spoofed and authentic signals received by UAVs. In the proposed methodology, several ML algorithms are deployed in order to select a suitable classification algorithm. To achieve the desired task, we have used GPS signal characteristics as features. Based on the feature specifications, our proposed model detects whether the signal is sent by the attacker or a legitimate entity. Moreover, to enhance the accuracy of the proposed work, we have developed different ML models using K-fold analyses by selecting different values of K-fold. These K-learning models are then used for voting purposes. For that, we have used soft and hard voting to assign the class to the unseen or test data. Different experiments and analyses were conducted to evaluate the strength of the proposed model. Moreover, a comparison of the proposed work with the existing work is also carried out which clearly shows that the proposed model works better than the existing ones.

As the proposed model is based on different ML algorithms, a decent accuracy is achieved. For further improvement in the proposed work, ML algorithms can be replaced with deep learning (DL) algorithms or a combination of both ML and DL algorithms. Moreover, In the future, DL strategies can be integrated with a convolution Neural Network (CNN).

REFERENCES

[1] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in *Proc. 10th USENIX Workshop Offensive Technol. (WOOT)*, 2016, pp. 1–11.

[2] Z. Li, Y. Lu, Y. Shi, Z. Wang, W. Qiao, and Y. Liu, "A Dyna-Q-based solution for UAV networks against smart jamming attacks," *Symmetry*, vol. 11, no. 5, p. 617, May 2019.

[3] Z. Zhen, P. Zhu, Y. Xue, and Y. Ji, "Distributed intelligent self-organized mission planning of multi-UAV for dynamic targets cooperative search-attack," *Chin. J. Aeronaut.*, vol. 32, no. 12, pp. 2706–2716, Dec. 2019.

[4] J. M. O. Barth, J.-P. Condomines, J.-M. Moschetta, A. Cabarbaye, C. Join, and M. Fliess, "Full model-free control architecture for hybrid UAVs," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 71–78.

[5] G. Vasconcelos, R. S. Miani, V. C. Guizilini, and J. R. Souza, "Evaluation of dos attacks on commercial Wi-Fi-based UAVs," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 212–223, 2019.

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navigat. Observ.*, vol. 2012, pp. 1–16, Jul. 2012.

[7] F. Dovis, *GNSS Interference Threats and Countermeasures*. Norwood, MA, USA: Artech House, 2015.

[8] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI matrice 100 quadcopter," *J. Global Positioning Syst.*, vol. 16, no. 1, pp. 1–11, Dec. 2018.
[9] D. He, Y. Qiao, S. Chen, X. Du, W. Chen, S. Zhu, and M. Guizani, "A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles," *IEEE Netw.*, vol. 33, no. 2, pp. 146–151, Mar. 2019.
[10] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.
[11] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver GPS spoofing detection: Error models and realization," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl.*, Dec. 2016, pp. 237–250.
[12] V. Chamola, P. Kotesh, A. A. Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, Feb. 2021, Art. no. 102324.
[13] M. Blanke and D. T. Nguyen, "Fault tolerant position-mooring control for offshore vessels," *Ocean Eng.*, vol. 148, pp. 426–441, Jan. 2018.
[14] J. Chung, "An accuracy study of RTK GNSS positioning applied to comparing maps for bentgrass habitat modeling," Tech. Rep., 2017.
[15] A. Broumandan and G. Lachapelle, "Spoofing detection using GNSS/INS/odometer coupling for vehicular navigation," *Sensors*, vol. 18, no. 5, p. 1305, Apr. 2018.
[16] L. Zhang, C. Sun, H. Zhao, W. Feng, C. Lei, and H. Liu, "The derivation and evaluation of algorithm of anti-spoofing attack on loosely/tightly coupled GNSS/INS integration system," in *Proc. China Satell. Navigat. Conf.* Singapore: Springer, 2020, pp. 691–700.
[17] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, p. 1433, May 2018.
[18] K. Jansen and C. Pöpper, "Advancing attacker models of satellite-based localization systems: The case of multi-device attackers," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2017, pp. 156–159.
[19] Y. Qiao, Y. Zhang, and X. Du, "A vision-based GPS-spoofing detection method for small UAVs," in *Proc. 13th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2017, pp. 312–316.
[20] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.
[21] W. Qin, M. T. Gamba, E. Falletti, and F. Dovis, "An assessment of impact of adaptive notch filters for interference removal on the signal processing stages of a GNSS receiver," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 5, pp. 4067–4082, Oct. 2020.
[22] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of UAVs through GPS spoofing," in *Proc. Global Wireless Summit (GWS)*, Nov. 2018, pp. 21–26.
[23] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 469–475, Feb. 2019.
[24] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 560–565.
[25] I. G. Ferrão, S. A. da Silva, D. F. Pigatto, and K. R. L. J. C. Branco, "GPS spoofing: Detecting GPS fraud in unmanned aerial vehicles," in *Proc. Latin Amer. Robot. Symp. (LARS), Brazilian Symp. Robot. (SBR) Workshop Robot. Educ. (WRE)*, Nov. 2020, pp. 1–6.
[26] X. Huang, Y. Tian, Y. He, E. Tong, W. Niu, C. Li, J. Liu, and L. Chang, "Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence," *Secur. Commun. Netw.*, vol. 2020, pp. 1–15, Dec. 2020.
[27] Y. Dang, C. Benzaïd, Y. Shen, and T. Taleb, "GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.
[28] L. Meng, S. Ren, G. Tang, C. Yang, and W. Yang, "UAV sensor spoofing detection algorithm based on GPS and optical flow fusion," in *Proc. 4th Int. Conf. Cryptography, Secur. Privacy*, Jan. 2020, pp. 146–151.
[29] D. Mendes, N. Ivaki, and H. Madeira, "Effects of GPS spoofing on unmanned aerial vehicles," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2018, pp. 155–160.
[30] X. Lu, D. Xu, L. Xiao, L. Wang, and W. Zhuang, "Anti-jamming communication game for UAV-aided VANETs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.
[31] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based DoS attack-resilient control framework for real-time UAV systems," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 1222–1227.
[32] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.
[33] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 1–31, May 2016.
[34] P. Dhomane and R. Mathew, "Counter-measures to spoofing and jamming of drone signals," Tech. Rep., 2020.
[35] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Proc. Infotech@ Aerosp.*, 2012, p. 2438.
[36] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Feb. 2017.
[37] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.
[38] R. Mitchell and I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 44, no. 5, pp. 593–604, May 2014.
[39] D. Muniraj and M. Farhood, "Detection and mitigation of actuator attacks on small unmanned aircraft systems," *Control Eng. Pract.*, vol. 83, pp. 188–202, Feb. 2019.
[40] L. Xiao, C. Xie, M. Min, and W. Zhuang, "User-centric view of unmanned aerial vehicle transmission against smart attacks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3420–3430, Apr. 2018.
[41] X. Huang, L. Shi, and J. A. K. Suykens, "Support vector machine classifier with pinball loss," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 5, pp. 984–997, May 2014.
[42] B. Scholkopf and A. J. Smola, *Learning With Kernels: Support Vector Machines, Regularization, Optimization, and Beyond* (Adaptive Computation and Machine Learning Series). 2018.
[43] Y. Li, S. Zahran, Y. Zhuang, Z. Gao, Y. Luo, Z. He, L. Pei, R. Chen, and N. El-Sheimy, "IMU/magnetometer/barometer/mass-flow sensor integrated indoor quadrotor UAV localization with robust velocity updates," *Remote Sens.*, vol. 11, no. 7, p. 838, Apr. 2019.
[44] F. Ke, J. Wang, M. Tu, X. Wang, X. Wang, X. Zhao, and J. Deng, "Characteristics and coupling mechanism of GPS ionospheric scintillation responses to the tropical cyclones in Australia," *GPS Solutions*, vol. 23, no. 2, p. 34, Apr. 2019.
[45] I. Cherniak and I. Zakharenkova, "New advantages of the combined GPS and GLONASS observations for high-latitude ionospheric irregularities monitoring: Case study of June 2015 geomagnetic storm," *Earth, Planets Space*, vol. 69, no. 1, pp. 1–14, Dec. 2017.
[46] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *J. Navigat.*, vol. 71, no. 1, pp. 169–188, Jan. 2018.
[47] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I," *Sensors*, vol. 20, no. 4, p. 1171, 2020.
[48] M. Sun, Y. Qin, J. Bao, and X. Yu, "GPS spoofing detection based on decision fusion with a K-out-of-N rule," *IJ Netw. Secur.*, vol. 19, no. 5, pp. 670–674, 2017.
[49] D. G. Silva, L. C. Oliveira, and M. Andrea, "Jitter estimation algorithms for detection of pathological voices," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, pp. 1–9, Dec. 2009.
[50] J. P. Teixeira, C. Oliveira, and C. Lopes, "Vocal acoustic analysis—Jitter, shimmer and HNR parameters," *Procedia Technol.*, vol. 9, pp. 1112–1122, Jan. 2013.
[51] J. P. Teixeira, D. Ferreira, and S. M. Carneiro, "Análise acústica vocalde-terminação do jitter e shimmer para diagnóstico de patalogias da fala," in *Proc. 6th Congresso Luso-Moçambicano Engenharia, 3rd Congresso Engenharia Moçambique*, 2011.

[52] S. Semanjski, A. Muls, I. Semanjski, and W. De Wilde, "Use and validation of supervised machine learning approach for detection of GNSS signal spoofing," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2019, pp. 1–6.
[53] F. Gallardo and A. P. Yuste, "SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection," *IEEE Access*, vol. 8, pp. 85515–85532, 2020.
[54] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *Proc. 23rd Int. Conf. Automat. Comput. (ICAC)*, Sep. 2017, pp. 1–11.
[55] E. M. D. L. Pinto, R. Lachowski, M. E. Pellenz, M. C. Penna, and R. D. Souza, "A machine learning approach for detecting spoofing attacks in wireless sensor networks," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 752–758.
[56] S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent detection algorithm against UAVs' GPS spoofing attack," in *Proc. IEEE 26th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2020, pp. 382–389.

ARSLAN SHAFIQUE received the B.E. degree in mechatronics and electrical engineering from Wah Engineering College, in 2014, and the M.S. degree in mechatronics and electrical engineering from Heavy Industries Taxila Education City (HITEC) University, Pakistan, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. He is serving as a Research Associate with the Faculty of Engineering and Applied Sciences, Riphah International University. His research interests include cryptography, secure communication, and machine learning.

ABID MEHMOOD (Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Australia. He is currently an Assistant Professor with Abu Dhabi University. His research interests include information security and privacy, data mining, machine learning, and cloud computing.

MOURAD ELHADEF (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from the Institute Supérieur de Gestion, Tunis, Tunisia, and the Ph.D. degree in computer science from the University of Sherbrooke, QC, Canada. He is currently a Professor of computer science with the College of Engineering, Abu Dhabi University, United Arab Emirates. He has over 50 publications in refereed journals and conference proceedings. His current research interests include fault tolerance and fault diagnosis in distributed, wireless and *ad-hoc* networks, cloud computing, artificial intelligence, and security. He is an Active Reviewer for various international conferences and journals, such as IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS and *Journal of Parallel and Distributed Computing*.