Received 20 October 2022; revised 9 November 2022; accepted 25 November 2022. Date of publication 1 December 2022; date of current version 14 December 2022.

*Digital Object Identifier 10.1109/OJCOMS.2022.3225846*

# Physical Layer Authentication for Satellite Communication Systems Using Machine Learning

**MOHAMMED ABDRABOU AND T. AARON GULLIVER**

Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 2Y2, Canada

CORRESPONDING AUTHOR: M. ABDRABOU (e-mail: abdrabou@uvic.ca)

**ABSTRACT** The vertical heterogeneous network (VHetNets) architecture aims to provide global connectivity for a variety of services by combining terrestrial, aerial, and space networks. Satellites complement cellular networks to overcome coverage and reliability limitations. However, the services of low-earth orbit (LEO) satellites are vulnerable to spoofing attacks. Physical layer authentication (PLA) can provide robust satellite authentication using machine learning (ML) with physical attributes. In this paper, an adaptive PLA scheme is proposed using Doppler frequency shift (DS) and received power (RP) features with a one-class classification support vector machine (OCC-SVM). One class-classification is a ML technique for outlier and anomaly detection which uses only legitimate satellite training data. This scheme is evaluated for fixed satellite services (FSS) and mobile satellite services (MSS) at different altitudes. Results are presented which show that the proposed scheme provides a higher authentication rate (AR) using DS and RP features simultaneously compared to other approaches in the literature.

**INDEX TERMS** Doppler frequency shift, received power, physical layer authentication, one-class classification, machine learning, support vector machine, vertical heterogeneous network.

## I. INTRODUCTION

FIFTH generation (5G) cellular networks have been developed to provide lower latency, higher speeds, and greater capacity than 4G networks. However, high deployment costs limit cellular network coverage in remote and rural areas. Moreover, natural disasters affect the reliability of cellular network infrastructure and can result in isolation [1]. Future wireless network architectures are being developed to improve coverage and reliability. This can be achieved by integrating terrestrial networks, e.g., cellular networks, and non-terrestrial aerial networks, e.g., unmanned aerial vehicle (UAV), aircraft, marine, and space networks [2]. This integration creates what is called a vertical heterogeneous network (VHetNet) or space-air-ground integrated network (SAGIN). The goal is to provide reliable connectivity worldwide [3], [4], [5].

The VHetNet architecture is composed of space, air, and ground networks. The space network includes geosynchronous equatorial orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO) satellites as well as inter-satellite links, ground stations, and terminals. The aerial network is composed of high-altitude platforms (HAPs), low-altitude platforms (LAPs), aircraft, UAVs, airships, and balloons, while the ground network consists of mobile ad hoc networks (MANETs) and cellular networks [2].

Satellite communications has become important for broadcast and broadband coverage in commercial, emergency, and military applications [6]. In particular, LEO satellite constellations have gained increasing attention for future networks because they are capable of providing global coverage. LEO satellite constellations are deployed at an altitude of 500 to 2000 km from Earth. They have low cost and low latency, and can provide fixed satellite services (FSS) and mobile satellite services (MSS).

The number of LEO satellites is increasing rapidly to provide the services required by VHetNets [1]. LEO constellations now provide global connectivity through thousands of satellites [7]. For instance, OneWeb has now launched 394 of 648 satellites to deliver low latency, high-speed global coverage by the end of 2022 [8]. SpaceX [9] and Amazon [10] are now interested in satellite-based systems [11]. However, the open nature of VHetNets makes satellite communication systems more vulnerable to active attacks such as spoofing. These attacks are considered a serious threat as they can

allow illegitimate satellites to send incorrect or malicious information to users [6], [12]. Physical layer authentication (PLA) can be used with upper layer authentication (ULA) schemes to strengthen network security [7] and provide robust satellite identification and authentication.

### A. RELATED WORK

A comprehensive survey on the security challenges for satellite communication systems was presented in [11]. Many satellite systems currently send unauthenticated messages or messages that have been authenticated at the application layer using symmetric key (implicit authentication) or public key solutions. Thus, simple and effective solutions to detect spoofing attacks are required. Several anti-spoofing schemes have been developed, e.g., global navigation satellite system (GNSS) spoofing detection [13], [14], received signal correlation using multiple antennas at the receiver [15], examining physical information such as received power, carrier-to-noise ratio (CNR), and angle of arrival [16], [17], leveraging ad-hoc network infrastructure [18], [19], and dedicated hardware [20], [21].

In [12], it was shown that satellite communications are vulnerable to spoofing attacks, especially the downlink satellite system information signalling (SIS). Thus, a PLA scheme was proposed to check satellite legitimacy using the Doppler frequency shift (DS). It is employed before initial access to the land mobile satellite (LMS) system so it is impossible for a spoofer to imitate the real-time DS of users. The high mobility of LEO satellites results in significant DS in the received signal [22]. The DS can be estimated either through signal observations or user calculations from satellite broadcast ephemeris. In terrestrial networks, physical layer attributes such as the channel state information (CSI) can be used for PLA [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]. However, CSI-based schemes may not be suitable for satellite authentication because of the line-of-sight (LOS) channel which does not provide sufficiently unique features.

In [34], Iridium LEO satellite signatures were obtained using the in-phase and quadrature (IQ) signal values. The signals from these satellites exhibit unique attenuation and fading characteristics due to the high mobility of up to 25000 km/h. The proposed scheme employs a convolutional neural network (CNN) for authentication, and pattern recognition techniques are used to generate synthetic images from the IQ values. In [35], [36], the DS of spacecraft links was used to generate symmetric keys. In [37], an orbit-based authentication scheme for downlink satellite communications was proposed. Satellites orbiting the Earth on a fixed trajectory provide a priori information for security purposes and time difference of arrival (TDOA) measurements from multiple receivers are used for satellite authentication.

A PLA scheme using DS was proposed in [7] for LEO satellites. Since velocity and location information for all satellites is available, LEO satellites can easily calculate reference DS values for any satellite. Thus, each satellite in a constellation can compare the measured DS with the reference value for the legitimate satellite in the constellation and make a decision on whether the satellite is legitimate or illegitimate. Then, a majority vote is taken at a fusion center to make the final authentication decision. In [38], a game theoretic PLA scheme was proposed for UAVs. The received signal strength (RSS) was used in the hypothesis test to discriminate between legitimate and illegitimate UAVs.

### B. CONTRIBUTIONS

Robust authentication is required for LEO satellite constellations which are a component of VHetNets. Consequently, this paper provides an authentication scheme based on physical layer features to authenticate satellites using machine learning (ML). In particular, an adaptive PLA scheme is proposed that employs a one-class classification support vector machine (OCC-SVM) using the DS and received power (RP) as features. The proposed scheme is evaluated using linear and polynomial OCC-SVM kernels. It is shown that a high authentication rate (AR) can be obtained using these features simultaneously. The contributions of this work are as follows.

- An adaptive PLA scheme using DS and RP features with OCC-SVM is proposed to authenticate LEO satellites.
- The proposed scheme is validated for FSS and MSS when the illegitimate satellites are within the FSS or MSS receive antenna half power beamwidth (HPBW).
- The missed detection rate (MDR), false alarm rate (FAR), and AR are evaluated using DS and RP features separately and simultaneously.
- Results are presented using two-line element (TLE) orbital data for real satellites [39] which verify the effectiveness of the proposed scheme.

The rest of the paper is organized as follows. Section II presents the system model. Section III introduces OCC-SVM and the proposed scheme is given in Section IV. Section V provides the evaluation metrics and the performance evaluation results are presented in Section VI. Finally, some concluding remarks are given in Section VII.

## II. SYSTEM MODEL

The system model for the LEO satellite PLA scheme is illustrated in Figure 1. The FSS or MSS station (FMS) must authenticate the legitimate satellite (Alice) over the entire communication session while preventing spoofing attacks from illegitimate satellites (Eves). The communication session starts from the lowest elevation angle ($\theta$) where the DS is maximum and the RP is minimum. A LEO satellite communication session is the time over which the satellite is continuously serving a given ground user [40]. A communication session is assumed to have $2n-1$ phases (time instances), and Figure 1 shows the first $n$ phases. We assume an attack scenario such that the Eves are very close to Alice so they are at the same altitude as Alice and within the FMS receive antenna HPBW. The FMS authenticates

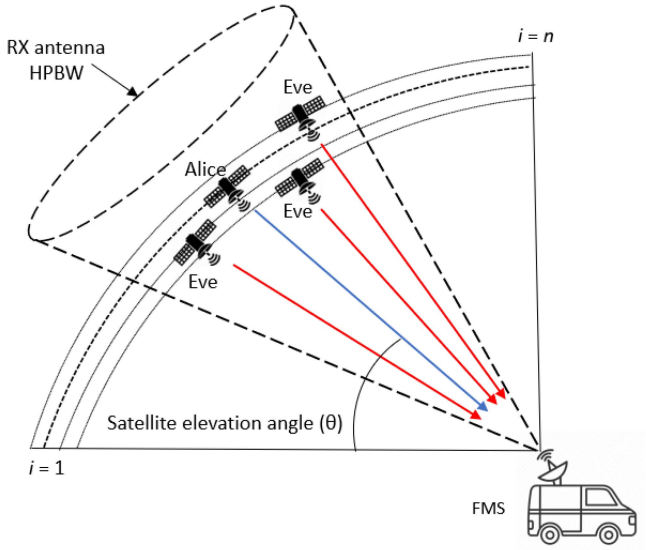


**FIGURE 1.** System model.

Alice using PLA over the communication session after ULA.

The proposed scheme is employed on the downlink and is divided into an initial phase and subsequent phases. In the initial phase, ULA authentication is performed and OCC-SVM training is conducted using the DS and RP features of Alice. In subsequent phases, OCC-SVM testing is conducted to establish the legitimacy of the received signals which could be from Alice or Eve. Therefore, the features in these phases are considered to be from an unknown user $U$ where $U \in \{\text{Alice}, \text{Eve}\}$. If the test is passed, the FMS decides the signal is from Alice so the training features are updated and OCC-SVM training is repeated. Conversely, if the test is failed, the FMS decides the signal is from Eve and the connection is terminated. The system tool kit (STK), which is a link budget analysis tool, is used with real satellite TLE orbital data to obtain the DS and RP. These values are employed to evaluate the effectiveness of the proposed authentication scheme.

### A. DOPPLER FREQUENCY SHIFT

The received signal at the FMS will have a DS given by [41]

$$f_d = \frac{v \times f_c}{c} \times \cos(\phi), \tag{1}$$

where $v$ is the velocity of the satellite, $c$ is the speed of light, $f_c$ is the center frequency, and $\phi$ is the angle between the satellite to FMS link and the direction of motion of the satellite. Consequently, for the same $v$ and $f_c$, at a given time, $\phi$ will differ between satellites so the DS is unique to a satellite.

### B. RECEIVED POWER

The RP at the FMS in watts is given by [42]

$$p_r = \frac{p_t \; g_t \; g_r}{(4\pi d/\lambda)^2}, \tag{2}$$

where $p_t$ is the transmitted power, $g_t$ is the gain of the transmit antenna, $g_r$ is the gain of the receive antenna, $d$ is the distance between transmitter and receiver, and $\lambda$ is the wavelength. The term $(4\pi d/\lambda)^2$ is known as the free space path loss (FSPL). The gain of the receive antenna in the direction $\theta$ is defined as $g_r(\theta)$ [43]. The angle $\theta$ is usually in the direction of the maximum gain, called the boresight direction of the antenna. It is used for FMS antenna tracking of the trajectory of Alice. Eve will not have the same trajectory and location as Alice at a given time. Thus, the RP from Eve at the FMS will differ from the corresponding RP from Alice due to the difference in $\theta$. Further, the FSPL for different satellites will differ due to the distance from the satellite to the FMS. It is assumed that the Eves have the same values of $p_t$ and $g_t$ as Alice which can be considered worst case.

### C. PROBLEM FORMULATION

In the initial phase, the DS and RP are obtained after ULA for the location of Alice at the start of the session. Then, the DS and the RP in subsequent phases are obtained by the FMS. Over this session, the signals from Alice and Eve are directed towards the FMS. Eve does this to imitate Alice. However, the FMS is following the trajectory of Alice over the communication session which is known. The FMS must decide between the two hypotheses

$$\begin{cases} \mathcal{H}_0 : \text{Alice transmits}, \\ \mathcal{H}_1 : \text{Eve transmits}. \end{cases} \tag{3}$$

Thus, the null hypothesis ($\mathcal{H}_0$) denotes that the signal is from Alice while the alternative hypothesis ($\mathcal{H}_1$) means that it is from Eve.

OCC-SVM training in the initial phase determines the authentication boundary for the features from Alice. In subsequent phases, OCC-SVM testing is conducted to determine if the corresponding features are located within this boundary. The user is accepted as legitimate if this test is passed. On the other hand, if the test decision is outside the boundary, the satellite is rejected. Furthermore, the OCC-SVM authentication boundary is updated in each subsequent phase to provide robust authentication.

## III. ONE-CLASS CLASSIFICATION SUPPORT VECTOR MACHINE (OCC-SVM)

One-class classification (OCC) is a ML technique that can be used to solve authentication problems. OCC is used to distinguish between Eve features and Alice features using training data from Alice. The proposed authentication framework employs the OCC-SVM algorithm, which is an extension of the two-class classification support vector machine (TCC-SVM) [44]. The goal with OCC-SVM is to find the optimal

authentication boundary that encloses most of the training data from Alice [24], [45], [46]. The method in [47] is used to solve the OCC problem using SVM. OCC-SVM computes a decision function $f$ which encloses most of the training data [24], [48].

First, the following optimization problem is solved [47], [48]

$$\min_{\mathbf{w},\mathbf{s},\rho} \ \frac{1}{2}\|\mathbf{w}\|^2 + \frac{1}{\eta\ell}\sum_{i=1}^{\ell} s_i - \rho,$$
$$\text{subject to} \ \ \mathbf{w}\cdot\Phi(\mathbf{g}_i) \geq \rho - s_i, \quad s_i \geq 0 \tag{4}$$

where $\mathbf{w}$ is the weight vector, $\rho$ is the distance from the origin to the boundary [24], $\ell$ is the number of training samples, $\Phi$ is the feature mapping, $\mathbf{g}_i$ is the $i$th feature vector, $s_i$ is the corresponding slack variable, and $\eta$ is the percentage of data considered as outliers [24]. OCC-SVM maps data to a feature space using kernels and then separates the features using a boundary. The optimization problem in (4) provides $\mathbf{w}$ and $\rho$ which determine the boundary used in the decision function (9). Using Lagrange multipliers $p_i, q_i \geq 0$ to solve (4) gives [47]

$$L(\mathbf{w},\mathbf{s},\mathbf{p},\mathbf{q},\rho) = \frac{1}{2}\|\mathbf{w}\|^2 + \frac{1}{\eta\ell}\sum_{i=1}^{\ell} s_i - \rho$$
$$-\sum_{i=1}^{\ell} p_i(\mathbf{w}\cdot\Phi(\mathbf{g}_i) - \rho + s_i) - \sum_{i=1}^{\ell} q_i s_i. \tag{5}$$

Setting the derivatives with respect to $\mathbf{w}$, $\mathbf{s}$ and $\rho$ equal to zero gives [47]

$$p_i = \tfrac{1}{\eta\ell} - q_i \leq \tfrac{1}{\eta\ell}, \tag{6}$$
$$\sum_{i=1}^{\ell} p_i = 1, \tag{7}$$
$$\mathbf{w} = \sum_{i=1}^{\ell} p_i\Phi(\mathbf{g}_i), \tag{8}$$

The decision function used to test a new sample $\mathbf{t}$ is [24], [48]

$$f(\mathbf{t}) = \text{sgn}(\mathbf{w}\cdot\Phi(\mathbf{t}) - \rho), \tag{9}$$

and substituting $\mathbf{w}$ from (8) gives

$$f(\mathbf{t}) = \text{sgn}\left(\sum_i p_i\Phi(\mathbf{g}_i)\cdot\Phi(\mathbf{t}) - \rho\right). \tag{10}$$

The kernel expansion is defined as [47]

$$k(\mathbf{g}_i,\mathbf{t}) = \Phi(\mathbf{g}_i)\cdot\Phi(\mathbf{t}) \tag{11}$$

so the decision function is

$$f(\mathbf{t}) = \text{sgn}\left(\sum_i p_i k(\mathbf{g}_i,\mathbf{t}) - \rho\right). \tag{12}$$

This will be positive for most samples in the training set and a new sample will pass if $f(\mathbf{t}) > 0$ and fail otherwise. The linear and polynomial kernels are considered in the proposed scheme. The linear kernel is

$$k(\mathbf{g}_i,\mathbf{t}) = \mathbf{g}_i\cdot\mathbf{t}, \tag{13}$$

and the polynomial kernel is [49]

$$k(\mathbf{g}_i,\mathbf{t}) = (\mathbf{g}_i\cdot\mathbf{t} + r)^d, d > 1, \tag{14}$$

where $d$ and $r$ are the degree and coefficient of the polynomial, respectively.

## IV. PROPOSED AUTHENTICATION SCHEME

In a real system, Alice will deviate from the reference trajectory [50] which will affect the signal received at the FMS station [51]. It is impossible for Eve to determine this deviation so Eve cannot manipulate her DS and RP values to imitate Alice. The proposed authentication scheme employs OCC-SVM using the DS and RP as features for training and testing.

Figure 2 presents a flowchart of the proposed scheme. In the initial phase $T_1$, after ULA authentication, data is collected from Alice for OCC-SVM training. The data legitimacy in this phase is guaranteed via higher layer protocols, e.g., international telecommunication union (ITU) standard authentication protocols. Then, in subsequent phases data from $U$ is employed by the FMS for testing and training. If the test is passed in a given phase, the corresponding data is used to update the features for training. A sliding window is used for this update so the oldest data is discarded. On the other hand, if the test fails, the connection is terminated.

The data vectors have the form

$$\mathbf{m} = [s\ p] \tag{15}$$

where $s$ and $p$ are the DS and RP, respectively. In phase $T_1$, Alice is first authenticated through ULA. Then, $\ell$ data vectors from Alice

$$\mathbf{d}_i = [s_i\ p_i], i = 1, 2, \ldots, \ell, \tag{16}$$

are scaled and used for OCC-SVM training to determine the boundary for authentication. In subsequent phases, OCC-SVM is used to test (after scaling), new data vectors

$$\mathbf{b} = [s\ p]_U, \tag{17}$$

from an unknown user $U$ using (12), where $U$ could be Alice or Eve. If the test is passed, the satellite is accepted, the features are updated, and OCC-SVM training is repeated. However, if the test fails, the connection is terminated.

Figure 3 shows the sliding window update process for the data where the rows are the data vectors. In phase $T_1$, the training data from Alice is a matrix with dimensions $\ell \times 2$. Then, in phase $T_2$ a new data vector $\mathbf{b}$ is tested (after scaling), and if accepted the data matrix is updated by discarding the first row $\mathbf{d}_1$ and adding the new data vector as row $\ell + 1$.

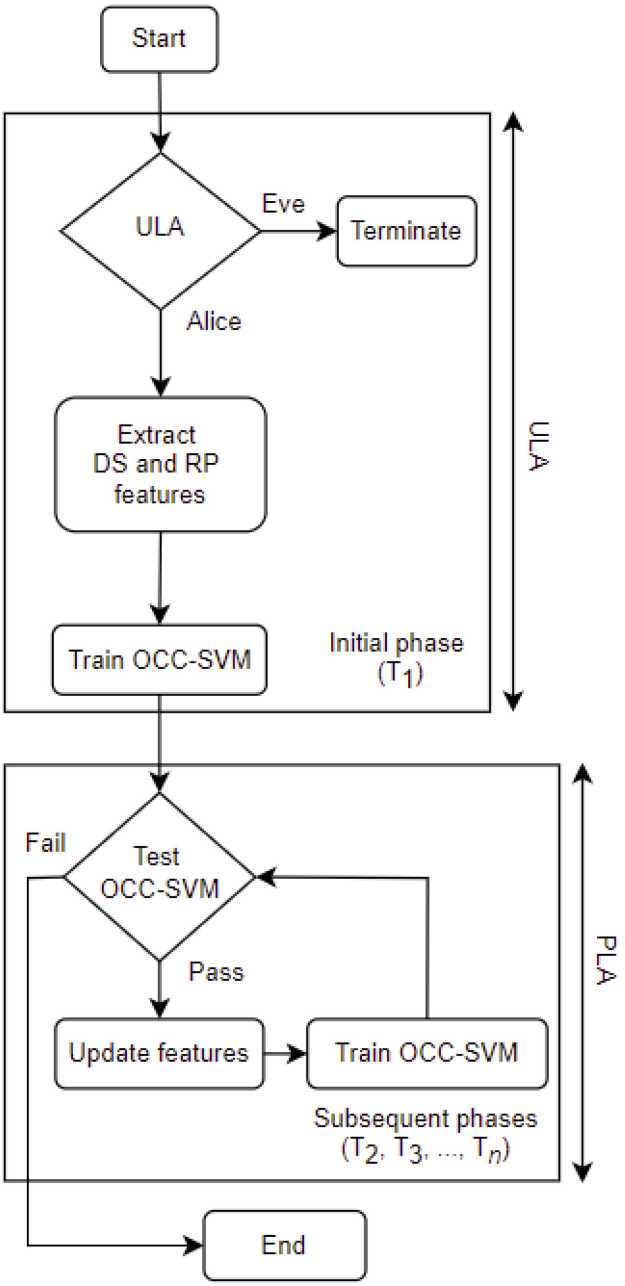


FIGURE 2. Proposed authentication scheme flowchart.

Thus, if the first $e$ new data vectors are accepted, the training data matrix is

$$\mathbf{M}_e = \begin{bmatrix} \mathbf{d}_{1+e} \\ \mathbf{d}_{2+e} \\ \vdots \\ \mathbf{d}_{\ell+e} \end{bmatrix}, \tag{18}$$

as shown in Figure 3 so $\ell$ vectors are used for training in each phase.

Min-Max scaling is separately applied to each feature. At the lowest $\theta$, the DS is maximum $s_{\max}$ and the RP is minimum $p_{\min}$, while at the highest $\theta$, the DS is minimum

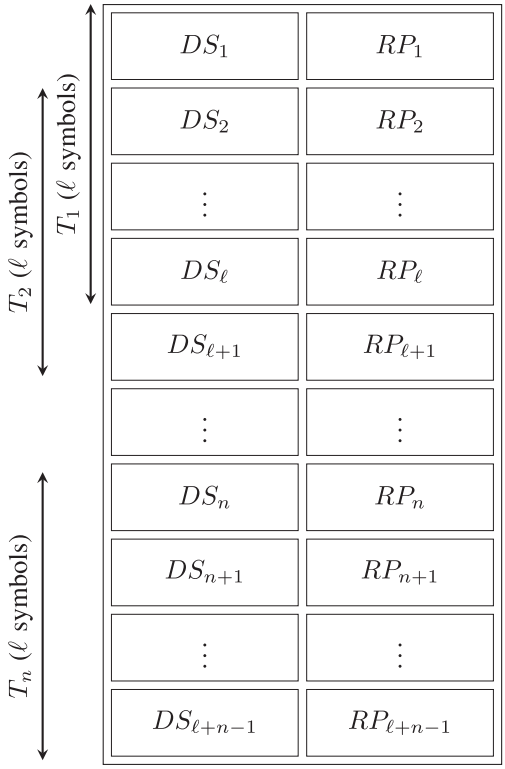


FIGURE 3. Sliding window for feature updates.

$s_{\min}$ and the RP is maximum $p_{\max}$. These values are based on satellite orbit and trajectory data available using STK [52]. The data vectors $\mathbf{d}_i$ are scaled as follows

$$s'_i = \frac{s_i - s_{\min}}{s_{\max} - s_{\min}}, \tag{19}$$

$$p'_j = \frac{p_j - p_{\min}}{p_{\max} - p_{\min}}, \tag{20}$$

so the corresponding feature vectors are

$$\mathbf{g}_i = [s'_i \; p'_i]. \tag{21}$$

The matrix of training vectors is then

$$\mathbf{G}_e = \begin{bmatrix} \mathbf{g}_{1+e} \\ \mathbf{g}_{2+e} \\ \vdots \\ \mathbf{g}_{\ell+e} \end{bmatrix} \tag{22}$$

The new data vector $\mathbf{b}$ is scaled to obtain the testing vector

$$\mathbf{t} = [s' \; p']_U. \tag{23}$$

The proposed scheme is summarized in Algorithm 1.

## V. EVALUATION METRICS

The confusion matrix shown in Figure 4 is used to evaluate the performance of the proposed scheme. True positive (TP) denotes correctly accepting Alice

$$f(\mathbf{t}|\text{Alice}) > 0,$$

**Algorithm 1** The Proposed Authentication Scheme

**Authenticate** Alice through ULA.
**Obtain** $s$ and $p$.
**Perform** Min-Max scaling to obtain $\mathbf{g}_i$ (21).
**Form** the training matrix $\mathbf{G}_e$ in (22).
**Train** OCC-SVM.
**Test t** using OCC-SVM (23).
**while** $(f(\mathbf{t}) > 0)$ **do**
  **Update** the training matrix $\mathbf{G}_e$.
  **Retrain** OCC-SVM.
  **Test t** using OCC-SVM (23).
**end while**

| Confusion Matrix | Predict Negative | Predict Positive |
|---|---|---|
| Actual Negative | TN $\mathcal{H}_1$ | FP Type II error |
| Actual Positive | FN Type I error | TP $\mathcal{H}_0$ |

**FIGURE 4.** Confusion matrix.

true negative (TN) denotes correctly rejecting Eve

$$f(\mathbf{t}|\text{Eve}) \leq 0,$$

false negative (FN) denotes incorrectly rejecting Alice

$$f(\mathbf{t}|\text{Alice}) \leq 0,$$

and false positive (FP) denotes incorrectly accepting Eve

$$f(\mathbf{t}|\text{Eve}) > 0.$$

The goal of PLA is to make the number of FN and FP low. The metrics used for performance evaluation are MDR, FAR, and AR which are given by

$$\text{MDR} = \frac{FP}{FP + TN}, \tag{24}$$

$$\text{FAR} = \frac{FN}{FN + TP}, \tag{25}$$

$$\text{AR} = \frac{TP + \gamma \times TN}{(TP + FN) + \gamma \times (TN + FP)}, \tag{26}$$

respectively, where $TP$, $TN$, $FN$, and $FP$ are the number of TP, TN, FN, and FP, and

$$\gamma = \frac{TP + FN}{TN + FP}, \tag{27}$$

is used to balance between Alice and the Eves.

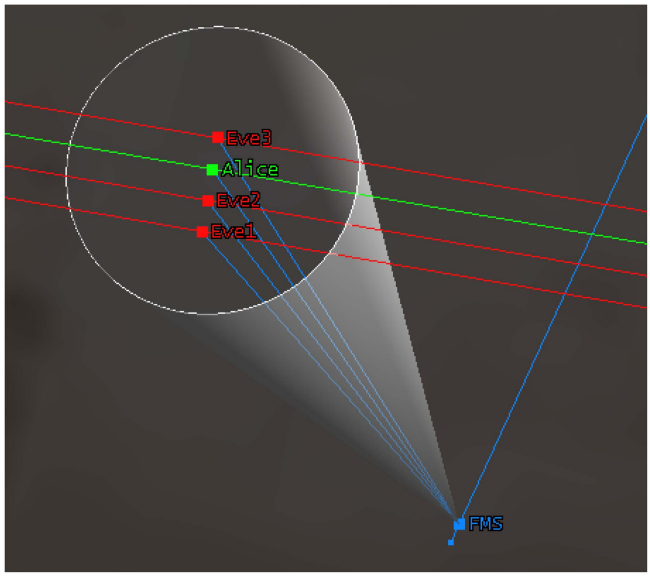


**FIGURE 5.** Simulation model.

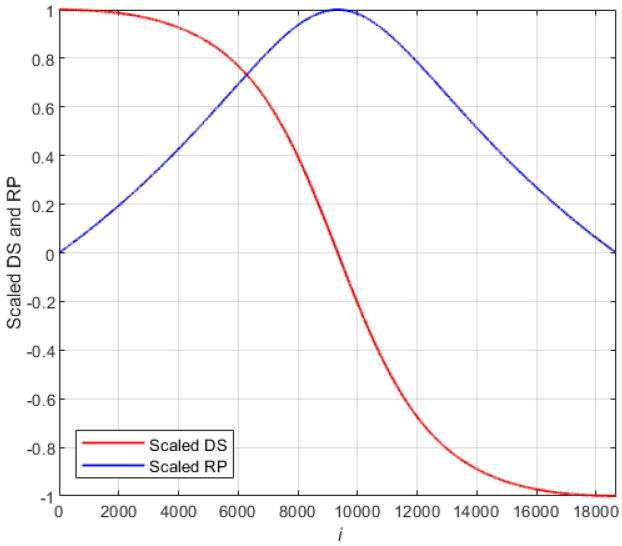


**FIGURE 6.** Scaled Doppler frequency shift and scaled received power over the communication session.

## VI. PERFORMANCE EVALUATION

In this section, the proposed scheme is evaluated using STK with the scikit-learn library in Python for linear and polynomial kernel OCC-SVM. STK is used to obtain the DS and RP values along the trajectories of Alice and Eve using (1) and (2). The simulation model is shown in Figure 5 and two scenarios are considered. The first is on-pause communications which refers to FSS where a fixed ground station authenticates Alice using a receive antenna 1.5 m in diameter. The second is on-move communications which refers to MSS where a mobile vehicle authenticates Alice using a receive antenna 0.5 m in diameter. A worst-case situation is considered where all Eve satellites are very close to Alice

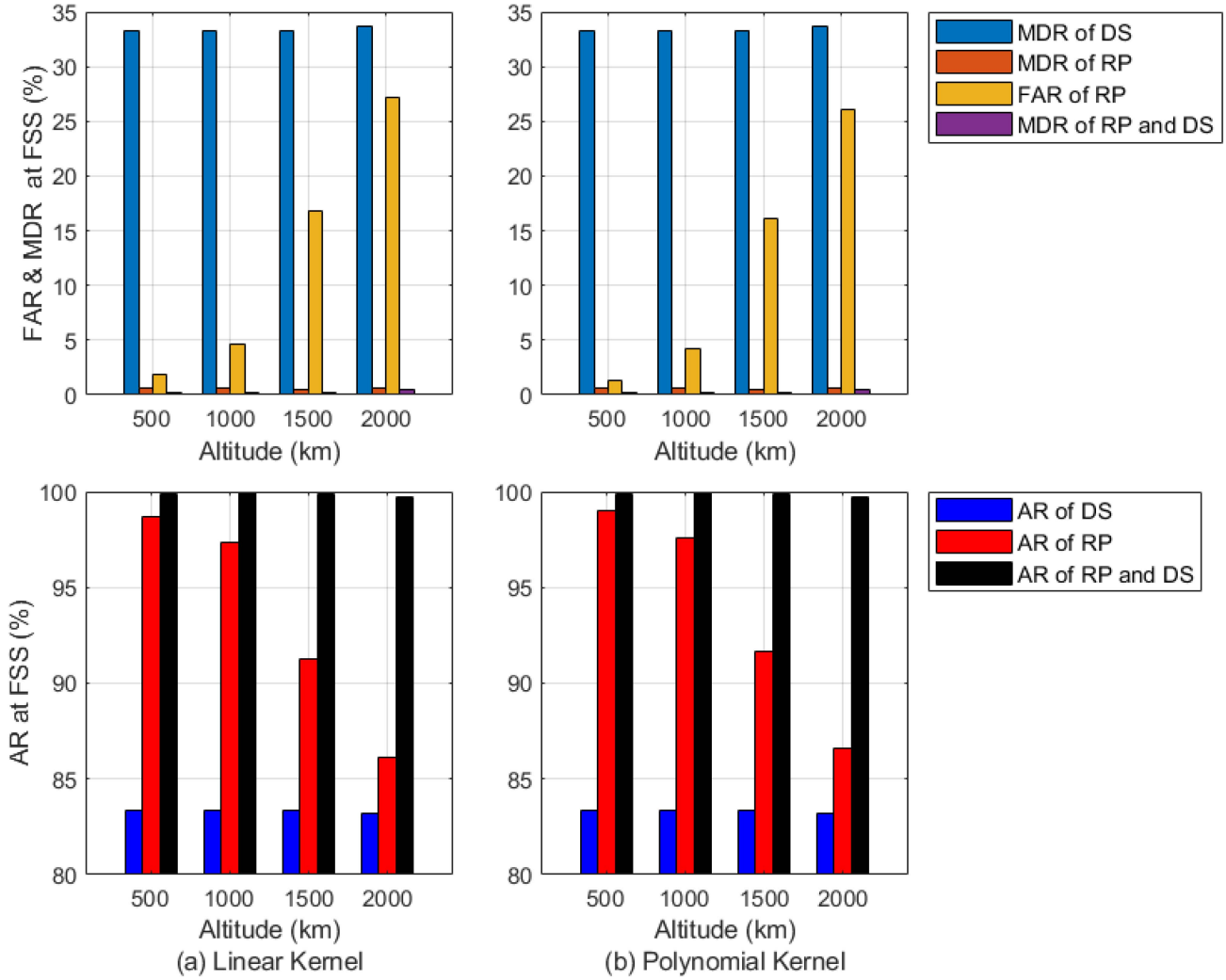


**FIGURE 7.** MDR, FAR, and AR versus altitude for FSS using DS, RP, and DS and RP features with (a) linear OCC-SVM kernel and (b) polynomial OCC-SVM kernel.

**TABLE 1.** Maximum distances between Alice and the Eves over the session at different altitudes.

| Altitude | Alice - Eve1 | Alice - Eve2 | Alice - Eve3 |
|---|---|---|---|
| 500 km | 10 km | 6 km | 6 km |
| 1000 km | 12 km | 7 km | 7 km |
| 1500 km | 13 km | 8 km | 8 km |
| 2000 km | 14 km | 8.5 km | 8.5 km |

with the same altitude and within the FMS receive antenna HPBW as shown in Figure 5.

The maximum distances between Alice and the Eves over the session in both scenarios are given in Table 1. The simulation parameters are given in Table 2 and $\gamma = \frac{1}{3}$ as there are 3 Eves. A BPSK signal model is considered with a 7.5 GHz center frequency and bandwidth $B = 10$ MHz. The transmit power for all satellites is 10 dBW at all altitudes. A line of sight (LOS) channel is assumed between the FMS and satellites with path loss exponent 2 and additive white Gaussian noise (AWGN) [53]. The receiver noise power is $KTB$ where $K$ is Boltzmann's constant and $T = 290$ K is the noise temperature. Figure 6 presents the scaled DS and scaled RP for Alice at an altitude of 2000 km. This shows that the scaled values in the first half of the communication session are similar to those in the second half. Thus, only DS and RP values for the first half of the session, i.e., phases $i = 1$ to $n$, are considered in the simulations.

### A. FIXED SATELLITE SERVICES

Figure 7 presents the MDR, FAR, and AR versus altitude for FSS utilizing OCC-SVM with linear and polynomial kernels for DS, RP, and DS and RP features. The FAR of DS and DS and RP for linear and polynomial OCC-SVM kernels is 0 and so is not shown in the figure.

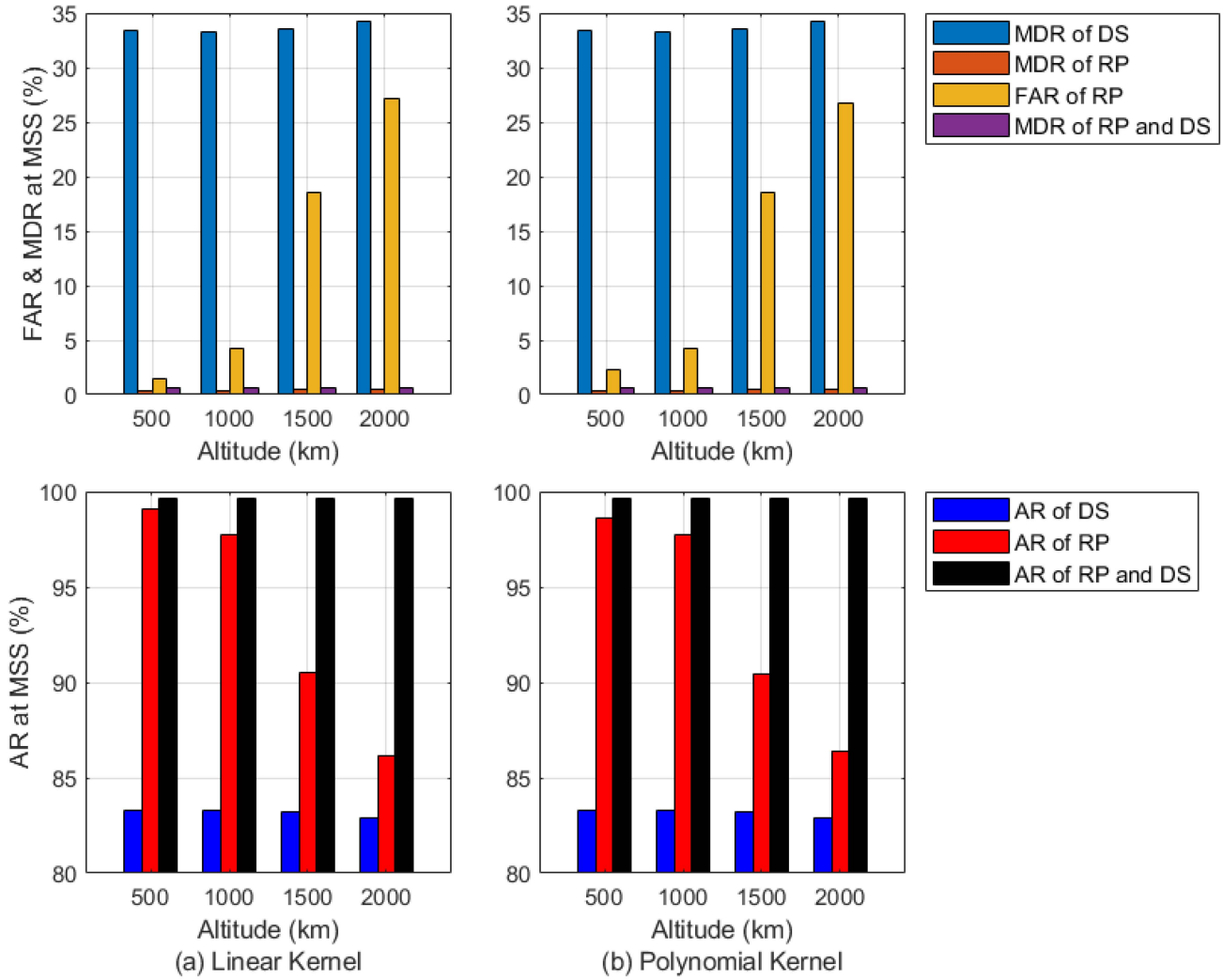


**FIGURE 8.** MDR, FAR, and AR versus altitude for MSS using DS, RP, and DS and RP features with (a) linear OCC-SVM kernel and (b) polynomial OCC-SVM kernel.

Figure 7a gives the MDR, FAR, and AR with the linear kernel. The MDR of DS is 33.3% at all altitudes and the AR is 83.3% at all altitudes. The MDR of RP is 0.67% at all altitudes while the FAR of RP is 1.9% at 500 km and increases to 27.1% at 2000 km. Thus, the AR of RP decreases with increasing altitude from 98.7% at 500 km to 86.1% at 2000 km. The MDR with both DS and RS is between 0.2% and 0.5% at all altitudes, and the corresponding AR is between 99.7% and 99.9%. Figure 7b presents the MDR, FAR, and AR for the polynomial kernel. This shows that the variations are smaller than with the linear kernel with an AR between 99.7% and 99.9%. However, the performance with the linear and polynomial kernels is similar at all altitudes. Further, using both DS and RP in the proposed scheme provides the highest AR which exceeds 99.7% for FSS.

### B. MOBILE SATELLITE SERVICES

Figure 8 gives the MDR, FAR, and AR versus altitude for MSS utilizing OCC-SVM with linear and polynomial kernels for DS, RP, and DS and RP features. The receive antenna diameter is 0.5 m so the HPBW is wider than in the FSS case. The FMS is moving in the direction shown in Figure 5. The FAR of DS and DS and RP for linear and polynomial kernels is 0 as in the FSS case and so is not shown in the figure.

Figure 8a gives the MDR, FAR, and AR with the linear kernel. The MDR with DS is slightly higher than in the FSS case. The AR is 83.0% at all altitudes. The MDR of RP also differs slightly and is 0.45% at all altitudes. In addition, the FAR of RP increases with increasing altitude. It is 1.4% at 500 km and increases to 27.1% at 2000 km. The AR of RP decreases with increasing altitude from 99.0% at 500 km to 86.1% at 2000 km. Finally, the MDR when using both DS and RS is slightly higher than in the FSS case, 0.65% at all altitudes. The results in Figure 8 show that the performance with the linear and polynomial kernels is similar for all altitudes. Moreover, using both DS and RP in the proposed scheme provides an AR which is greater than 99.6%. In summary, the proposed scheme achieves an AR greater than 99.6% for FSS and MSS at all altitudes

**TABLE 2.** Simulation parameters.

| Parameter | Value |
|---|---|
| Frequency Band | C Band |
| Center frequency | 7.5 GHz |
| Modulation | BPSK |
| Bandwidth | 10 MHz |
| Data rate | 10 Mbps |
| FSS antenna diameter | 1.5 m |
| MSS antenna diameter | 0.5 m |
| Satellite altitudes | 500, 1000, 1500, and 2000 km |
| Tx power for all satellites | 10 dBW |

with OCC-SVM using both DS and RP features and linear or polynomial kernels.

### C. DISCUSSION

The DS and RP are used as features in the ML algorithm because they are affected by the altitude and position of the satellites. Thus, they can be considered unique for a satellite and so are suitable for authentication purposes. For both FSS and MSS, the DS provides similar authentication performance at all altitudes. Conversely, for a constant transmit power, the RP performance decreases with altitude. However, using both the DS and RP provides the highest authentication performance for all altitudes and there is only a minimal decrease with altitude. Good performance is achieved even for the worst-case scenario shown in Figure 5 in which all Eves are very close to Alice, at the same altitude, and within the HPBW of the ground station.

## VII. CONCLUSION

The increase in the number of low earth orbit (LEO) satellite constellations makes vertical heterogeneous networks (VHetNets) a solution to provide worldwide wireless coverage. However, LEO satellites are vulnerable to spoofing attacks so an efficient and effective authentication scheme is needed. An adaptive physical layer authentication (PLA) scheme using machine learning (ML) was proposed to solve this problem using the Doppler frequency shift (DS) and received power (RP) as features. A one-class classification support vector machine (OCC-SVM) with linear and polynomial kernels was employed. Results were presented which show that a high authentication rate (AR) can be achieved for both fixed and mobile satellite services using the DS and RP as features. In particular, the AR in this case exceeds 99.6% for both services. Finally, the proposed scheme employing both the DS and RP as features was shown to be superior to using only the DS or RP as features as in [7] and [38], respectively.

## REFERENCES


[1] A. Guidotti et al., "Satellite-enabled LTE systems in LEO constellations," in *Proc. IEEE Int. Conf. Commun. Workshops*, Paris, France, 2017, pp. 876–881.

[2] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[3] G. K. Kurt et al., "A vision and framework for the high altitude platform station (HAPS) networks of the future," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 729–779, 2nd Quart., 2021.

[4] M. Alzenad and H. Yanikomeroglu, "Coverage and rate analysis for vertical heterogeneous networks (VHetNets)," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5643–5657, Dec. 2019.

[5] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "Physical layer security framework for optical non-terrestrial networks," 2021, *arXiv:2106.08197*.

[6] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C.-M. Chen, "A lightweight key agreement and authentication scheme for satellite-communication systems," *IEEE Access*, vol. 8, pp. 46278–46287, 2020.

[7] O. A. Topal and G. K. Kurt, "Physical layer authentication for LEO satellite constellations," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Austin, TX, USA, 2022, pp. 1952–1957.

[8] "OneWeb confirms successful launch of 36 satellites, after rapid year of progress." OneWeb. 2021. [Online]. Available: https://oneweb.net/resources/oneweb-confirms-successful-launch-36-satellites-after-rapid-year-progress

[9] M. Adam and P. Tereza. "Starlink: SpaceX's satellite Internet project." 2022. [Online]. Available: https://www.space.com/spacex-starlink-satellites.html

[10] P. Jon. "Facebook's satellite Internet team joins Amazon." 2021. [Online]. Available: https://www.theverge.com/2021/7/14/22576788

[11] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," 2021, *arXiv:2112.11324*.

[12] Q.-Y. Fu, Y.-H. Feng, H.-M. Wang, and P. Liu, "Initial satellite access authentication based on Doppler frequency shift," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 498–502, Mar. 2021.

[13] E. Schmidt, N. Gatsis, and D. Akopian, "A GPS spoofing detection and classification correlator-based technique using the LASSO," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 6, pp. 4224–4237, Dec. 2020.

[14] 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.

[15] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1794–1805, Aug. 2015.

[16] S. Bhamdipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *Proc. IEEE/ION Position Location Navig. Symp.*, Monterey, CA, USA, 2018, pp. 1485–1491.

[17] K. D. Wesson, B. L. Evans, and T. E. Humphreys, "A combined symmetric difference and power monitoring GNSS anti-spoofing technique," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Austin, TX, USA, 2013, pp. 217–220.

[18] G. Oligeri, S. Sciancalepore, and R. Di Pietro, "GNSS spoofing detection via opportunistic IRIDIUM signals," in *Proc. ACM Conf. Security Privacy Wireless Mobile Netw.*, Linz, Austria, 2020, pp. 42–52.

[19] E. Axell, E. G. Larsson, and D. Persson, "GNSS spoofing detection using multiple mobile COTS receivers," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, South Brisbane, QLD, Australia, 2015, pp. 3192–3196.

[20] D. Borio, "PANOVA tests and their application to GNSS spoofing detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 381–394, Jan. 2013.

[21] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.
[22] M. Mitry, "Routers in space: Kepler communications' CubeSats will create an Internet for other satellites," *IEEE Spectr.*, vol. 57, no. 2, pp. 38–43, Feb. 2020.
[23] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.
[24] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1506–1521, 2020.
[25] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5420–5432, Aug. 2020.
[26] M. Rezaee, P. J. Schreier, M. Guillaud, and B. Clerckx, "A unified scheme to achieve the degrees-of-freedom region of the MIMO interference channel with delayed channel state information," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1068–1082, Mar. 2016.
[27] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, "On the error region for channel estimation-based physical layer authentication over Rayleigh fading," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 941–952, 2015.
[28] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.
[29] Z. Jiang, J. Zhao, X.-Y. Li, J. Han, and W. Xi, "Rejecting the attack: Source authentication for Wi-Fi management frames using CSI information," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2544–2552.
[30] F. Formaggio and S. Tomasin, "Authentication of satellite navigation signals by wiretap coding and artificial noise," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, 2019, Art. no. 98.
[31] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 55–61, Oct. 2019.
[32] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Inf. Netw.*, vol. 5, no. 3, pp. 237–264, Sep. 2020.
[33] X. Qiu et al., "Wireless user authentication based on KLT and Gaussian mixture model," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Marrakesh, Morocco, 2019, pp. 1–5.
[34] G. Oligeri, S. Raponi, S. Sciancalepore, and R. Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," 2020, *arXiv:2010.05470*.
[35] O. A. Topal, G. K. Kurt, and H. Yanikomeroglu, "Securing the inter-spacecraft links: Doppler frequency shift based physical layer key generation," in *Proc. IEEE Int. Conf. Wireless Space Extreme Environ.*, Vicenza, Italy, 2020, pp. 112–117.
[36] O. A. Topal, G. K. Kurt, and H. Yanikomeroglu, "Securing the inter-spacecraft links: Physical layer key generation from Doppler frequency shift," *IEEE J. Radio Freq. Identif.*, vol. 5, pp. 232–243, 2021.
[37] E. Jedermann, M. Strohmeier, M. Schäfer, J. Schmitt, and V. Lenders, "Orbit-based authentication using TDOA signatures in satellite networks," in *Proc. ACM Conf. Security Privacy Wireless Mobile Netw.*, Abu Dhabi, UAE, 2021, pp. 175–180.
[38] Y. Zhou, P. L. Yeoh, K. J. Kim, Z. Ma, Y. Li, and B. Vucetic, "Game theoretic physical layer authentication for spoofing detection in UAV communications," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6750–6755, Jun. 2022.
[39] T. Kelso. "Celestrak orbit visualization." 2022. [Online]. Available: https://celestrak.org/NORAD/elements/supplemental/
[40] A. Al-Hourani, "Session duration between handovers in dense LEO satellite networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2810–2814, Dec. 2021.
[41] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[42] T. Pratt and J. E. Allnutt, *Satellite Communications*. New Delhi, India: Wiley, 2020.
[43] S. Silver, *Microwave Antenna Theory and Design*. New York, NY, USA: McGraw-Hill, 1949.
[44] A. Fernández, S. García, M. Galar, R. C. Prati, B. Krawczyk, and F. Herrera, *Learning from Imbalanced Data Sets*. Cham, Switzerland: Springer, 2018.
[45] D. M. Tax and R. P. Duin, "Support vector data description," *Mach. Learn.*, vol. 54, no. 1, pp. 45–66, 2004.
[46] M. Abdrabou and T. A. Gulliver, "Adaptive physical layer authentication using machine learning with antenna diversity," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6604–6614, Oct. 2022.
[47] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Comput.*, vol. 13, no. 7, pp. 1443–1471, 2001.
[48] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," *IEEE Access*, vol. 9, pp. 31595–31607, 2021.
[49] J. Amose, P. Manimegalai, C. Narmatha, and M. S. P. Raj, "Comparative performance analysis of kernel functions in support vector machines in the diagnosis of pneumonia using lung sounds," in *Proc. Int. Conf. Comput. Inf. Technol.*, Tabuk, Saudi Arabia, 2022, pp. 320–324.
[50] M. Murata, I. Kawano, and K. Inoue, "Precision onboard navigation for LEO satellite based on precise point positioning," in *Proc. IEEE/ION Position Location Navig. Symp.*, Portland, OR, USA, 2020, pp. 1506–1513.
[51] A. Hauschild, J. Tegedor, O. Montenbruck, H. Visser, and M. Markgraf, "Precise onboard orbit determination for LEO satellites with real-time orbit and clock corrections," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig.*, Portland, OR, USA, 2016, pp. 3715–3723.
[52] J. Zhang, G. Yang, Q. Xu, and Y. Zhao, "Application in radar simulation of STK/connect module," in *Proc. WRI World Congr. Comput. Sci. Inf. Eng.*, Los Angeles, CA, USA, 2009, pp. 274–276.
[53] J. Aldis and A. Burr, "Capacity of bandlimited phase only modulated systems in AWGN (satellite channels)," in *Proc. IEE Colloq. Adv. Modulation Coding Techn. Satell. Commun.*, London, U.K., 1992, pp. 6/1–6/5.

**MOHAMMED ABDRABOU** received the B.Sc. and M.Sc. degrees in electrical engineering from Military Technical College, Cairo, Egypt, in 2009 and 2016, respectively. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada. His research interests include wireless communications, physical layer authentication, cryptography, information theory, and machine learning.

**T. AARON GULLIVER** received the Ph.D. degree in electrical engineering from the University of Victoria, Victoria, BC, Canada, in 1989. From 1989 to 1991, he was a Defence Scientist with Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic appointments with Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999, where he is a Professor with the Department of Electrical and Computer Engineering. His research interests include wireless communications, information theory, intelligent networks, machine learning, cryptography, and security. From 2007 to 2012, he was an Editor and from 2012 to 2017, an Area Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He became a Fellow of the Engineering Institute of Canada in 2002, and a Fellow of the Canadian Academy of Engineering in 2012.