IEEE Open Journal of Vehicular Technology

Received 13 September 2022; accepted 24 October 2022.
Date of current version 30 November 2022. The review of this article was coordinated by Editor Lina Mohjazi.

Digital Object Identifier 10.1109/OJVT.2022.3218609

Authentication for Satellite Communication Systems Using Physical Characteristics

MOHAMMED ABDRABOU AND T. AARON GULLIVER

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

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

ABSTRACT Satellite communication networks have gained a lot of attention recently as a solution to mitigate the limitations of terrestrial networks such as stability and coverage. However, integrating satellite and terrestrial networks makes the system more vulnerable to spoofing attacks. Thus, robust and effective authentication is required. Physical layer authentication (PLA) has emerged as an alternative paradigm that uses physical characteristics to achieve authentication. In this paper, PLA is proposed for low earth orbit (LEO) satellites using the Doppler frequency shift (DS) and received power (RP) characteristics. Hypothesis testing using a threshold or machine learning (ML) is considered to discriminate between legitimate and illegitimate satellites. For ML, a one-class classification support vector machine (OCC-SVM) is employed which uses training data from only legitimate users. The performance is evaluated using real satellite data from the system tool kit (STK). Results are presented which show that the authentication rate (AR) with DS is higher than with RP at low elevation angles for both schemes, but is higher with RP at high elevation angles. Further, the ML authentication scheme provides a higher AR than the threshold scheme for a small percentage of the training data considered as outliers, but at larger percentages the OR threshold scheme is better.

INDEX TERMS Doppler frequency shift, physical layer authentication, received power, vertical heterogeneous network, space network, machine learning.

I. INTRODUCTION

The importance of terrestrial networks has increased tremendously in recent years due to advances such as the Internet of Things (IoT) and sixth-generation (6G) technologies. However, these networks have drawbacks such as limited coverage in remote and rural areas due to high deployment costs and network reliability degradation due to environmental factors and natural disasters [1]. 6G wireless network architectures are being developed to improve coverage and reliability [2]. This will include the integration of terrestrial networks, e.g. cellular networks, and non-terrestrial aerial networks, e.g. unmanned aerial vehicle (UAV), aircraft, marine, and space networks [3]. This integration creates what is called a vertical heterogeneous network (VHetNet), also known as a space-air-ground-sea integrated network (SAGSIN) [4], [5], [6]. VHetNets are widely envisioned as a promising 6G technology and thus VHetNet authentication has attracted significant research attention [7].

Satellite communications is important for many commercial, emergency, and military applications [8]. The number of low earth orbit (LEO) satellites which can deliver VHetNet services has increased significantly [1], and the thousands of LEO satellites now provide global connectivity [9]. For example, OneWeb has launched 394 of a planned 648 satellites to provide low latency, high-speed global coverage by the end of 2022 [10]. SpaceX [11] and Amazon [12] have both expressed interest in satellite-based communication systems [13]. However, the open nature of VHetNets makes satellite communication systems vulnerable to active attacks such as spoofing attacks. Spoofing attacks are regarded as a serious threat because they allow illegitimate satellites to send false or malicious data to users [8], [14]. Most satellite systems currently send unauthenticated messages or messages that have been authenticated at the application layer using symmetric or public key solutions. Using authentication for access control is an efficient way to ensure data security [15],

[16]. Thus, simple and effective solutions are required for these systems to improve network security [13]. This can be achieved by using physical layer authentication (PLA) in conjunction with upper layer authentication (ULA) schemes [9].

In [13], the security challenges for satellite communication systems were considered. Several anti-spoofing schemes have been developed, e.g. global navigation satellite system (GNSS) spoofing detection [17], [18], received signal correlation using multiple antennas at the receiver [19], examining physical information such as received power, carrier-to-noise ratio (CNR), and angle of arrival [20], [21], and leveraging ad-hoc network infrastructure [22], [23] and dedicated hardware [24], [25]. It was shown in [14] that satellite communications is vulnerable to spoofing attacks. Thus, a PLA scheme was proposed to validate satellites using the Doppler frequency shift (DS). It is used prior to initial access to the land mobile satellite (LMS) system so an attacker cannot imitate the real-time DS of a user. 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 [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36]. 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 [37], a PLA framework was proposed for controller area networks (CANs) to mitigate spoofing attacks. This scheme utilizes the arrival intervals and magnitudes of the received signals as features. Moreover, reinforcement learning (RL) is employed for authentication using the Dyna architecture.

In [38], Iridium LEO satellite signatures were obtained using 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 [39], [40], the DS of spacecraft links was used to generate symmetric keys. An orbit-based authentication scheme for satellite communications was proposed in [41]. 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 authentication. A PLA scheme using DS was proposed in [9] for LEO satellites. Since velocity and location information for all satellites is available, reference DS values for any satellite can easily be calculated. Thus, each satellite in a constellation can compare the measured DS value with the reference value for the satellite in the constellation to decide whether it is legitimate. Then, a majority vote is taken at a fusion center to make the final authentication decision.

A robust satellite authentication scheme is required due to the use of LEO satellites in VHetNets. Consequently, this paper presents PLA for these satellites using the DS and received power (RP) characteristics. Hypothesis testing using a threshold or machine learning (ML) is considered to discriminate between legitimate and illegitimate satellites. For ML, a one-class classification support vector machine (OCC-SVM) is used which is a technique for outlier and anomaly detection that uses only legitimate training data. The performance is evaluated using real satellite data from the system tool kit (STK) and DS and RP estimation errors are considered. The DS and RP are updated throughout the communication session to provide robust authentication. Results are presented which show that a high authentication rate (AR) can be obtained using these features. Further, at low elevation angles θ, the AR with DS is higher than with RP, while the converse is true at high θ. The contributions of this paper are as follows.

- An adaptive PLA scheme using DS and RP characteristics to authenticate LEO satellites is proposed.
- Hypothesis testing using a threshold or OCC-SVM is used to discriminate between legitimate and illegitimate satellites.
- The AR is evaluated using DS and RP characteristics separately and together over the communication session.
- Results are presented using two-line element (TLE) data for real satellites to verify the effectiveness of the proposed schemes. TLE data is orbital data for Earth-orbiting objects and is available at: https://celestrak.com/.

The rest of the paper is organized as follows. Section II presents the system model and Section III introduces OCC-SVM. The proposed authentication schemes are given in Section IV. Section V provides simulation results to evaluate the performance and some concluding remarks are given in Section VI.

II. SYSTEM MODEL

The system model for the LEO satellite PLA scheme is illustrated in Fig. 1. The fixed or mobile satellite services station (FMS) must authenticate the legitimate satellite (Alice) over the communication session while preventing spoofing attacks from an illegitimate satellite (Eve). Eve tries to imitate Alice in order to send incorrect or malicious data to users. The FMS first authenticates Alice using ULA and then PLA is performed over the session. A LEO satellite communication session is the time over which the satellite is continuously serving a given ground user [42]. A session is assumed to have $2n-1$ phases (time instances). Fig. 1 shows the first n phases.

ULA is performed in the initial phase and DS and RP values are obtained. In subsequent phases, PLA is performed at the FMS which must decide between the two hypotheses

$$\begin{cases} \mathcal{H}_0: & \text{Alice is transmitting,} \\ \mathcal{H}_1: & \text{Eve is transmitting.} \end{cases} \tag{1}$$

Thus, $\mathcal{H}_0$ denotes that the signal is from Alice while $\mathcal{H}_1$ means it is from Eve. If the test is passed, then the current DS and RP values are kept and used to test new DS and RP values in the next phase.

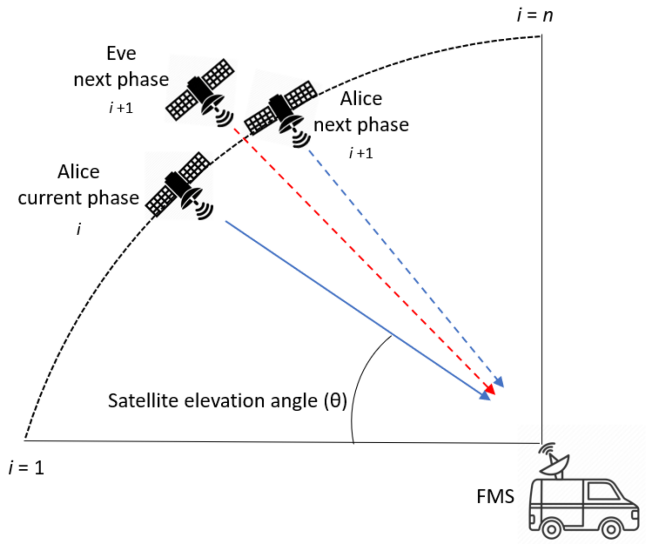

FIGURE 1. The system model.

A. DOPPLER FREQUENCY SHIFT

The received signal at the FMS will have a DS given by [43]

$$f_d = \frac{v \times f_c}{c} \times \cos(\phi), \tag{2}$$

where v is the velocity of the satellite, c is the speed of light, f_c is the center frequency, and ϕ 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, ϕ will differ between satellites so the DS is unique to a satellite.

B. RECEIVED POWER

The power received at the FMS in watts is given by [44]

$$p_r = \frac{p_t \; g_t \; g_r}{(4\pi l/\lambda)^2}, \tag{3}$$

where p_t is the transmit power, g_t is the gain of the transmit antenna, g_r is the gain of the receive antenna, l is the distance between the satellite and FMS, and λ is the wavelength. The term $(4\pi l/\lambda)^2$ is known as the free space path loss (FSPL).

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. The proposed authentication framework employs the OCC-SVM [45] algorithm to distinguish between Eve and Alice using training data from Alice. The goal with OCC-SVM is to find the optimal authentication boundary that surrounds most of the training data from Alice [46]. The method in [45] is used to solve the OCC problem using SVM. OCC-SVM computes a decision function f which encloses most of the training data [27]. A test sample $\mathbf{b}$ is accepted if $f(\mathbf{b}) > 0$ which indicates it is within the authentication boundary.

First, the following optimization problem is solved [45], [47]

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

where $\mathbf{w}$ is the weight vector, ρ is the distance from the origin to the boundary, ℓ is the number of training samples, Φ is the feature mapping, $\mathbf{g}_i$ is the ith feature vector, s_i is the corresponding slack variable, and η is the percentage of data considered as outliers. Using Lagrange multipliers $p_i, q_i \geq 0$ to solve (4) gives [45]

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

Setting the derivatives with respect to $\mathbf{w}$, $\mathbf{s}$ and ρ equal to zero gives [45]

$$p_i = \frac{1}{\eta\ell} - q_i \leq \frac{1}{\eta\ell}, \tag{6}$$

$$\sum_{i=1}^{\ell} p_i = 1, \tag{7}$$

$$\mathbf{w} = \sum_{i=1}^{\ell} p_i \Phi(\mathbf{g}_i). \tag{8}$$

The decision function used to test a new vector $\mathbf{b}$ is [27], [47]

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

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

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

The kernel expansion is defined as [45]

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

so the decision function is

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

The test is passed if $f(\mathbf{b}) > 0$ and fails otherwise. The linear kernel is considered in the proposed scheme and is given by

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

IV. AUTHENTICATION BASED ON PHYSICAL CHARACTERISTICS

Fig. 2 shows the authentication flowchart. In the initial phase, ULA is performed and DS and RP values are obtained at

Algorithm 1: Threshold authentication scheme.

Authenticate using ULA.
Collect DS and RP values from Alice.
Compute $T_{d,a,i}$ and $T_{r,a,i}$ using (20) and (21), respectively.
Test $T_{d,u,i+1}$ and $T_{r,u,i+1}$.
while Alice **do**
  Update the DS and RP values from Alice.
  Compute $T_{d,a,i}$ and $T_{r,a,i}$ using (20) and (21), respectively.
  Test $T_{d,u,i+1}$ and $T_{r,u,i+1}$.
end while

Algorithm 2: Machine learning authentication scheme.

Authenticate using ULA.
Collect DS and RP values from Alice.
Form the training matrix **M**.
Train using OCC-SVM.
Test using OCC-SVM.
while Alice **do**
  Update the training matrix **M**.
  Train using OCC-SVM.
  Test using OCC-SVM.
end while

the FMS. Then, the threshold is computed for the threshold authentication scheme or the OCC-SVM is trained for the ML authentication scheme. In subsequent phases, a threshold or OCC-SVM test is performed using new DS and RP values. If the test is passed, these values are kept and used to test the DS and RP values in the next phase, otherwise the connection is terminated. Note that it is intractable for Eve to reproduce the exact DS and RP values at the ground station corresponding to Alice.

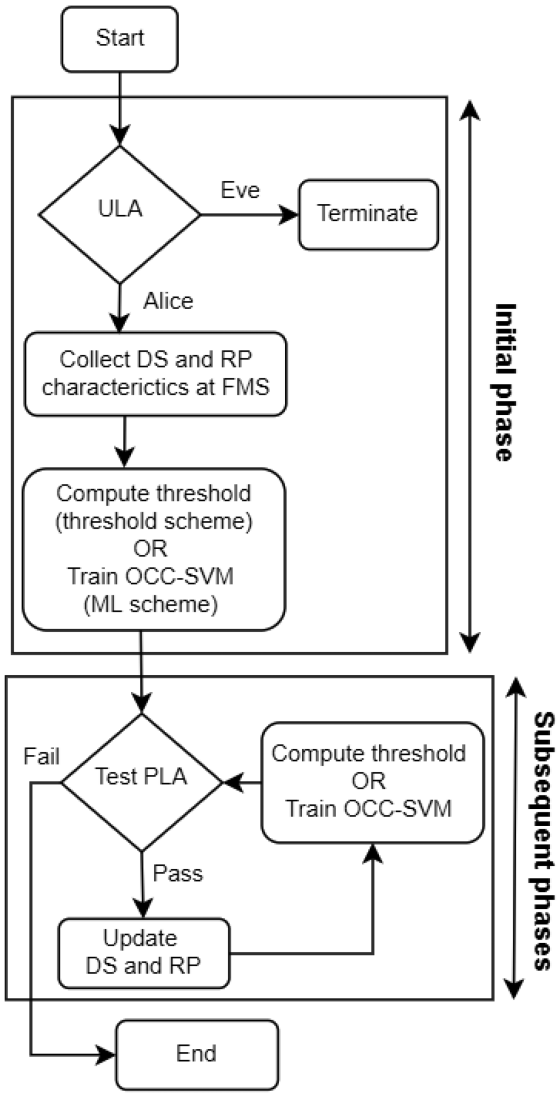

FIGURE 2. The authentication flowchart.

A. ESTIMATED DOPPLER FREQUENCY SHIFT

Let $\hat{f}_{d,a,i}$, $\hat{f}_{d,a,i+1}$, and $\hat{f}_{d,e,i+1}$ be the estimated DS at the FMS for Alice in the current phase, and Alice and Eve in the next phase, respectively. Then

$$\hat{f}_{d,a,i} = f_{d,a,i} + \varepsilon_{d_1}, \tag{14}$$

$$\hat{f}_{d,a,i+1} = f_{d,a,i+1} + \varepsilon_{d_2}, \tag{15}$$

$$\hat{f}_{d,e,i+1} = \alpha_{i+1} f_{d,a,i+1} + \varepsilon_{d_3}, \tag{16}$$

where $f_{d,a,i}$ and $f_{d,a,i+1}$ are the exact DS for Alice in the current and next phase, respectively, α_{i+1}, $0 < \alpha_{i+1} < 1$, is the ratio between the DS of Alice and Eve, and ε_{d_1}, ε_{d_2}, and ε_{d_3} are the DS estimation errors at the FMS due to factors such as approximation and receiver noise. The DS estimation errors can be modeled as Gaussian random variables with $\varepsilon_{d_1} \sim N(0, \sigma_{d_1}^2)$, $\varepsilon_{d_2} \sim N(0, \sigma_{d_2}^2)$, and $\varepsilon_{d_3} \sim N(0, \sigma_{d_3}^2)$ [14].

B. ESTIMATED RECEIVED POWER

Let $\hat{p}_{r,a,i}$, $\hat{p}_{r,a,i+1}$, $\hat{p}_{r,e,i+1}$ be the estimated RP at the FMS for Alice in the current phase, and Alice and Eve in the next phase, respectively. Then

$$\hat{p}_{r,a,i} = p_{r,a,i} + \varepsilon_{r_1}, \tag{17}$$

$$\hat{p}_{r,a,i+1} = p_{r,a,i+1} + \varepsilon_{r_2}, \tag{18}$$

$$\hat{p}_{r,e,i+1} = \beta_{i+1} p_{r,a,i+1} + \varepsilon_{r_3}, \tag{19}$$

where $p_{r,a,i}$ and $p_{r,a,i+1}$ are the exact RP for Alice in the current and next phase, respectively, β_{i+1}, $0 < \beta_{i+1} < 1$, is the ratio between the RP of Alice and Eve, and ε_{r_1}, ε_{r_2}, and ε_{r_3} are the RP estimation errors. The RP estimation errors can be modeled as Gaussian random variables with $\varepsilon_{r_1} \sim N(0, \sigma_{r_1}^2)$, $\varepsilon_{r_2} \sim N(0, \sigma_{r_2}^2)$, and $\varepsilon_{r_3} \sim N(0, \sigma_{r_3}^2)$ [48].

In a real system, Alice will have a deviation from the reference trajectory [49] which will affect the signal received at the

ground station [50]. It is impossible for Eve to determine this deviation and this will cause errors if Eve tries to manipulate her RP and DS values to imitate Alice. Further, the errors in the estimated DS and RP values at both Eve and Alice will make this task even more difficult.

C. THRESHOLD AUTHENTICATION SCHEME

In the threshold authentication scheme, the magnitudes of the differences between two consecutive DS and RP values are employed [27]. For Alice, these magnitudes are

$$T_{d,a,i} = |\hat{f}_{d,a,i+1} - \hat{f}_{d,a,i}|, \tag{20}$$

$$T_{r,a,i} = |\hat{p}_{r,a,i+1} - \hat{p}_{r,a,i}|, \tag{21}$$

respectively, and can be expected to be within small thresholds ϵ_d and ϵ_r. Therefore, the DS hypothesis test can be expressed as

$$\begin{cases} \mathcal{H}_0 : |T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d, \\ \mathcal{H}_1 : |T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d, \end{cases} \tag{22}$$

where $T_{d,u,i+1}$ is the DS magnitude from an unknown satellite which could be Alice or Eve. Similarly, the RP hypothesis test can be expressed as

$$\begin{cases} \mathcal{H}_0 : |T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r, \\ \mathcal{H}_1 : |T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r, \end{cases} \tag{23}$$

where $T_{r,u,i+1}$ is the RP magnitude from an unknown satellite which could be Alice or Eve. The AND hypothesis test for the DS and RP magnitudes is given by

$$\begin{cases} \mathcal{H}_0 : |T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d \text{ AND} \\ \qquad |T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r, \\ \mathcal{H}_1 : |T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d \text{ AND} \\ \qquad |T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r, \end{cases} \tag{24}$$

and the OR hypothesis test for these magnitudes is given by

$$\begin{cases} \mathcal{H}_0 : |T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d \text{ OR} \\ \qquad |T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r, \\ \mathcal{H}_1 : |T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d \text{ OR} \\ \qquad |T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r. \end{cases} \tag{25}$$

The AND and OR authentication schemes provide lower and upper bounds, respectively, on the performance so the performance of other schemes such as soft-decision fusion will lie between them. The threshold authentication scheme is summarized in Algorithm 1.

The false alarm rate (FAR), missed detection rate (MDR), and authentication rate (AR) are used to evaluate the authentication schemes. The FAR for the DS and RP threshold authentication schemes is defined as

$$FAR_{d,t} = P(|T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d | \mathcal{H}_0), \tag{26}$$

$$FAR_{r,t} = P(|T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r | \mathcal{H}_0), \tag{27}$$

respectively. The MDR for the DS and RP threshold authentication schemes is defined as

$$MDR_{d,t} = P(|T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d | \mathcal{H}_1), \tag{28}$$

$$MDR_{r,t} = P(|T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r | \mathcal{H}_1), \tag{29}$$

respectively. The FAR and MDR for the AND threshold authentication scheme are defined as

$$\begin{aligned} FAR_{\text{AND},t} = P(&|T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d \text{ AND} \\ &|T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r | \mathcal{H}_0), \end{aligned} \tag{30}$$

$$\begin{aligned} MDR_{\text{AND},t} = P(&|T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d \text{ AND} \\ &|T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r | \mathcal{H}_1), \end{aligned} \tag{31}$$

respectively. The FAR and MDR for the OR threshold authentication scheme are defined as

$$\begin{aligned} FAR_{\text{OR},t} = P(&|T_{d,u,i+1} - T_{d,a,i}| > \epsilon_d \text{ OR} \\ &|T_{r,u,i+1} - T_{r,a,i}| > \epsilon_r | \mathcal{H}_0), \end{aligned} \tag{32}$$

$$\begin{aligned} MDR_{\text{OR},t} = P(&|T_{d,u,i+1} - T_{d,a,i}| \leq \epsilon_d \text{ OR} \\ &|T_{r,u,i+1} - T_{r,a,i}| \leq \epsilon_r | \mathcal{H}_1), \end{aligned} \tag{33}$$

respectively. The AR for the DS, RP, AND, and OR threshold authentication schemes is given by

$$\text{AR}_{d,t} = \frac{1}{2} \times \left[(1 - FAR_{d,t}) + (1 - MDR_{d,t}) \right], \tag{34}$$

$$\text{AR}_{r,t} = \frac{1}{2} \times \left[(1 - FAR_{r,t}) + (1 - MDR_{r,t}) \right], \tag{35}$$

$$\text{AR}_{\text{AND},t} = \frac{1}{2} \times \left[(1 - FAR_{\text{AND},t}) + (1 - MDR_{\text{AND},t}) \right], \tag{36}$$

$$\text{AR}_{\text{OR},t} = \frac{1}{2} \times \left[(1 - FAR_{\text{OR},t}) + (1 - MDR_{\text{OR},t}) \right], \tag{37}$$

respectively.

D. MACHINE LEARNING AUTHENTICATION SCHEME

In the ML scheme, OCC-SVM is employed using DS, RP, or DS and RP as features for training and testing. In the initial phase, DS and RP values are collected from Alice for OCC-SVM training. Then, DS and RP values from an unknown satellite u, which could be Alice or Eve, are used for testing at the FMS. If the test is passed, the corresponding DS and RP values are used to update the features for training. On the other hand, if the test fails, the connection is terminated.

The DS and RP data vector has the form

$$\mathbf{m} = \begin{bmatrix} \hat{f}_{d,a,i} & \hat{p}_{r,a,i} \end{bmatrix}. \tag{38}$$

After Alice is authenticated via ULA, ℓ data vectors corresponding to ℓ samples from Alice

$$\mathbf{d}_j = \begin{bmatrix} \hat{f}_{d,a,i,j} & \hat{p}_{r,a,i,j} \end{bmatrix}, j = 1, 2, \ldots, \ell, \tag{39}$$

Confusion Matrix	Predict Negative	Predict Positive
Actual Negative (N)	TN $\mathcal{H}_1$	FP Type II error
Actual Positive (P)	FN Type I error	TP $\mathcal{H}_0$

FIGURE 3. Confusion matrix.

are used for OCC-SVM training. Then, OCC-SVM is used to test ℓ data vectors from u

$$\mathbf{b}_j = \left[\hat{f}_{d,u,i+1,j} \quad \hat{p}_{r,u,i+1,j}\right], j = 1, 2, \ldots, \ell. \tag{40}$$

If the test is passed the satellite is accepted, the features are updated, and OCC-SVM is retrained. Otherwise, the connection is terminated. The data matrix in phase $i-1$ is

$$\mathbf{M} = \begin{bmatrix} \mathbf{d_{i+1}} \\ \mathbf{d}_{i+2} \\ \vdots \\ \mathbf{d}_{i+\ell} \end{bmatrix}. \tag{41}$$

In the initial phase ($i = 1$), this data is from Alice and is used for training. The matrix in subsequent phases ($i > 1$) is first tested, and if the test is passed, the matrix is used for training in the next phase. The ML authentication scheme is summarized in Algorithm 2.

The confusion matrix shown in Fig. 3 is used to evaluate the performance of the ML authentication scheme. True positive (TP) denotes correctly accepting a legitimate satellite, true negative (TN) denotes correctly rejecting an illegitimate satellite, false negative (FN) denotes incorrectly rejecting a legitimate satellite, and false positive (FP) denotes incorrectly accepting an illegitimate satellite. The FAR for DS, RP, and DS and RP is given by

$$FAR_{d,l} = \frac{FN_d}{P}, \tag{42}$$

$$FAR_{r,l} = \frac{FN_r}{P}, \tag{43}$$

$$FAR_{d,r,l} = \frac{FN_{d,r}}{P}, \tag{44}$$

respectively, where FN_d, FN_r, and $FN_{d,r}$ are the FN for DS, RP, and DS and RP, respectively, and $P = TP + FN$. The MDR for DS, RP, and DS and RP is given by

$$MDR_{d,l} = \frac{FP_d}{N}, \tag{45}$$

TABLE 1. Simulation Parameters

Parameter	Value
Center frequency	7.5 GHz
Antenna diameter	0.5 m
Modulation	BPSK
Bandwidth	10 MHz
Data rate	10 Mbps
Satellite altitude	2000 km
Tx power for all satellites	10 dBW

TABLE 2. Range of Doppler Frequency Shifts At Different Altitudes

Altitude	Minimum	Maximum
500 km	0 Hz	165 kHz
1000 km	0 Hz	145 kHz
1500 km	0 Hz	130 kHz
2000 km	0 Hz	120 kHz

$$MDR_{r,l} = \frac{FP_r}{N}, \tag{46}$$

$$MDR_{d,r,l} = \frac{FP_{d,r}}{N}, \tag{47}$$

respectively, where FP_d, FP_r, and $FP_{d,r}$ are the FP for DS, RP, and DS and RP, respectively, and $N = TN + FP$. The AR for the DS, RP, and DS and RP when $P = N$ (equal amounts of data from Alice and Eve), is given by

$$AR_{d,l} = \frac{1}{2} \times \left[(1 - FAR_{d,l}) + (1 - MDR_{d,l})\right], \tag{48}$$

$$AR_{r,l} = \frac{1}{2} \times \left[(1 - FAR_{r,l}) + (1 - MDR_{r,l})\right], \tag{49}$$

$$AR_{d,r,l} = \frac{1}{2} \times \left[(1 - FAR_{d,r,l}) + (1 - MDR_{d,r,l})\right], \tag{50}$$

respectively.

V. SIMULATION RESULTS

In this section, the proposed authentication schemes are evaluated using real DS and RP values obtained using STK during the communication session along the satellite trajectories. DS and RP values are obtained every 0.01 s and $n = 9330$. The proposed ML authentication scheme employs OCC-SVM using the scikit-learn library in Python. The simulation parameters are given in Table 1.

A. DS AND RP OVER THE COMMUNICATION SESSION

Tables 2 and 3 give the range of DS and RP values, respectively, at different altitudes. The normalized Doppler

TABLE 3. Range of Received Power At Different Altitudes

Altitude	Minimum	Maximum
500 km	-110 dBW	-98 dBW
1000 km	-113 dBW	-102 dBW
1500 km	-115 dBW	-105 dBW
2000 km	-117 dBW	-108 dBW

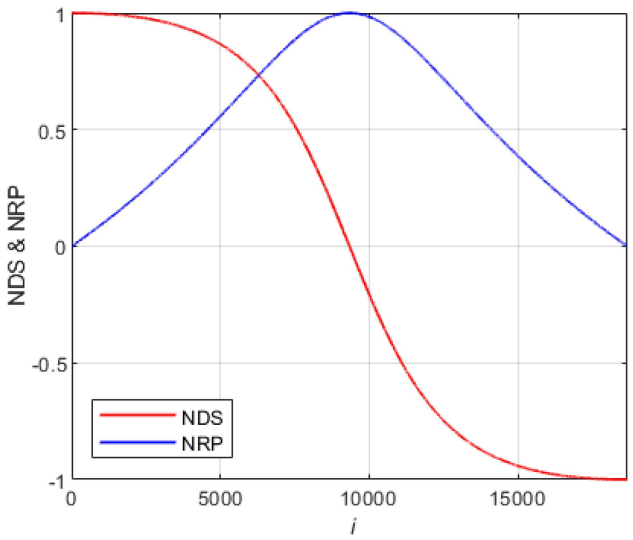

FIGURE 4. Normalized Doppler frequency shift (NDS) and normalized received power (NRP) over the communication session.

frequency shift (NDS) and normalized received power (NRP) over the communication session are defined as

$$NDS_i = \frac{DS_i}{\max(DS)}, i = 1, 2, \ldots, 2n-1, \quad (51)$$

$$NRP_i = \frac{RP_i}{\max(RP)}, i = 1, 2, \ldots, 2n-1, \quad (52)$$

respectively, where $\max(DS)$ and $\max(RP)$ are the corresponding maximum values. Fig. 4 presents the NDS and NRP for Alice at an altitude of 2000 km. This shows that the NDS and NRP values in the first half of the communication session are similar to those in the second half. Thus, only DS and RP values for phases 1 to n are considered in the simulations. The DS and RP ratios between Alice and Eve are given by

$$\alpha_i = \frac{f_{d,a,t_i}}{f_{d,e,t_i}}, i = 1, 2, \ldots, n, \quad (53)$$

$$\beta_i = \frac{p_{r,a,t_i}}{p_{r,e,t_i}}, i = 1, 2, \ldots, n, \quad (54)$$

respectively, and the corresponding normalized values are

$$N\alpha_i = \frac{\alpha_i}{\max(\alpha_i)}, i = 1, 2, \ldots, n, \quad (55)$$

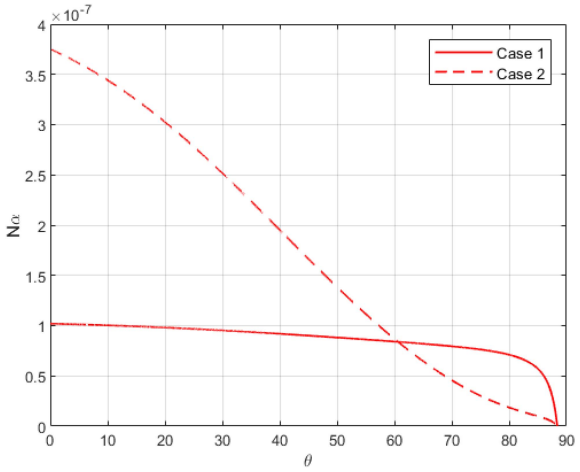

FIGURE 5. Normalized α_i ($N\alpha_i$) versus θ.

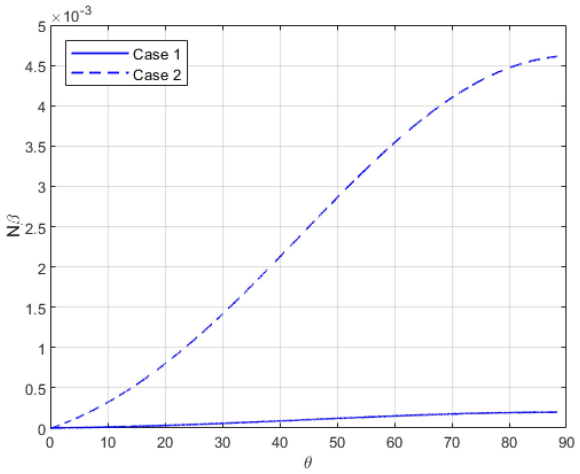

FIGURE 6. Normalized β_i ($N\beta_i$) versus θ.

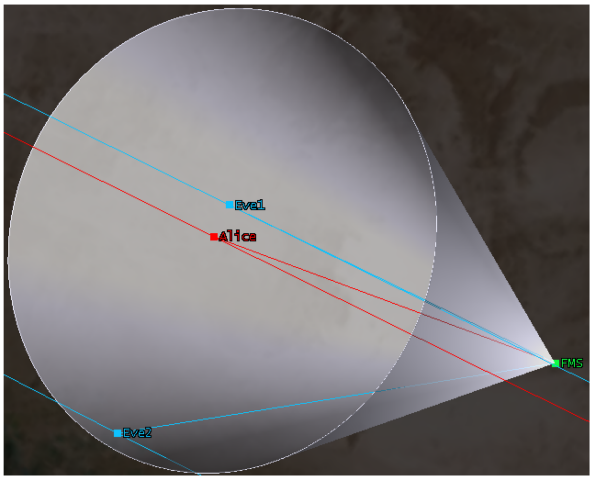

FIGURE 7. The trajectories for Eve and Alice where Eve1 corresponds to case 1 and Eve2 to case 2.

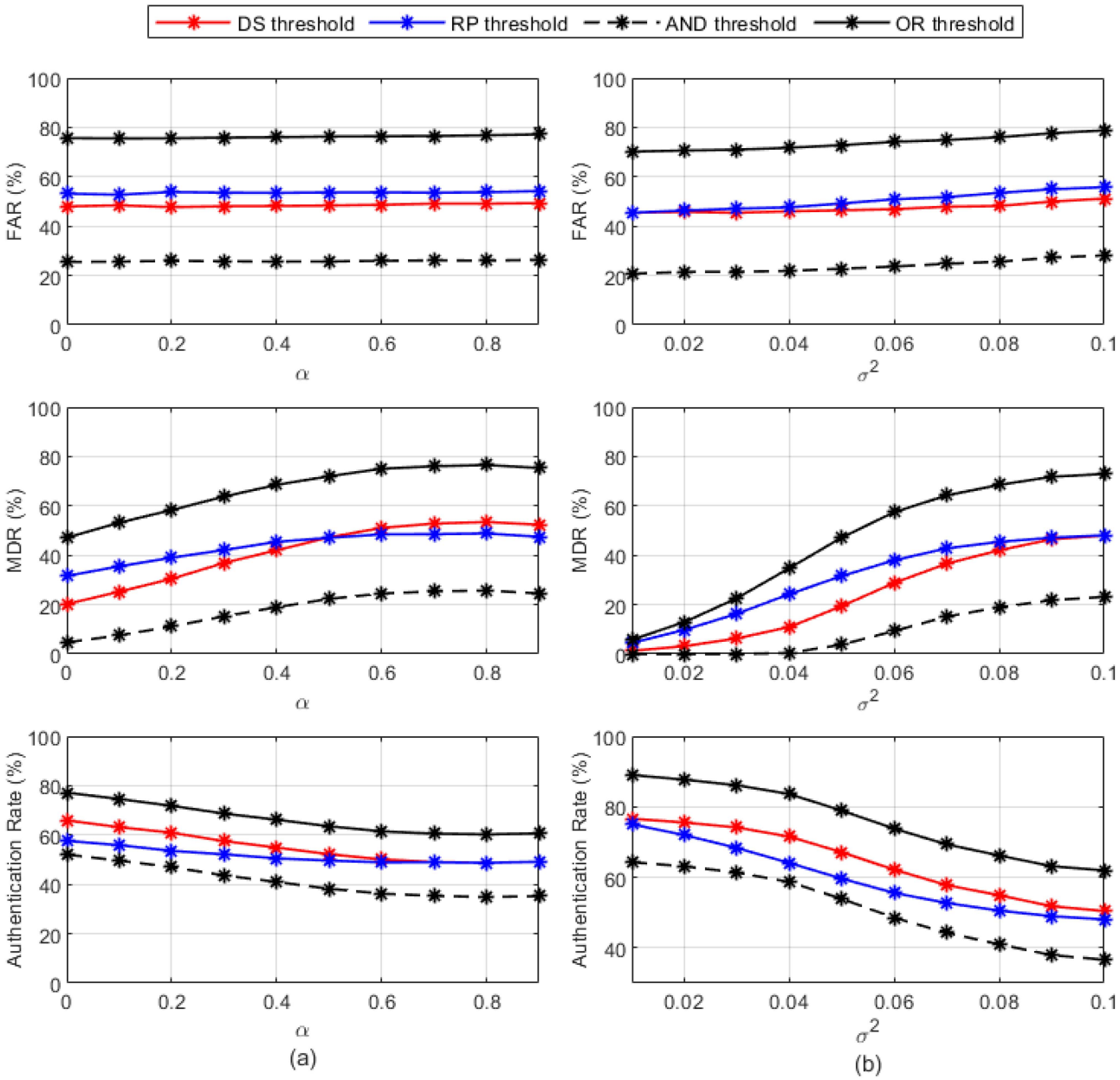

FIGURE 8. MDR, FAR, and AR for the DS, RP, AND, and OR threshold authentication schemes averaged over the communication session versus (a) α with $\sigma^2 = 0.08$, and (b) σ^2 with $\alpha = 0.4$.

$$N\beta_i = \frac{\beta_i}{\max(\beta_i)}, i = 1, 2, \ldots, n, \tag{56}$$

where $\max(\alpha_i)$ and $\max(\beta_i)$ are the maximum α_i and β_i, respectively. Figs. 5 and 6 show $N\alpha_i$ and $N\beta_i$, respectively, versus θ for two cases. In case 1, the DS and RP values are obtained for Alice and Eve when the trajectories are very close, while in case 2 the trajectories are far apart. However, in both cases Eve is within the half power beam width (HPBW) of the FMS receive antenna as indicated in Fig. 7. Figs. 5 and 6 show that the variations in $N\alpha_i$ and $N\beta_i$ are negligible in both cases. For example, the difference between the largest and smallest values of $N\alpha_i$ is 4×10^{-7} while the corresponding difference in $N\beta_i$ is less than 5×10^{-3}. Thus, it is assumed in the following that $\alpha_i = \alpha$ and $\beta_i = \beta$ over the communication session. In the simulations, $\sigma^2_{d_1} = \sigma^2_{d_2} = \sigma^2_{d_3} = \sigma^2_{r_1} = \sigma^2_{r_2} = \sigma^2_{r_3} = \sigma^2$, $\alpha_i = \beta_i = \alpha$, $\epsilon_d = 0.1 \times T_{d,a,i}$, and $\epsilon_r = 0.1 \times T_{r,a,i}$.

B. THRESHOLD AUTHENTICATION SCHEME PERFORMANCE

Figs. 8(a) and 8(b) present the MDR, FAR, and AR for the DS, RP, AND, and OR threshold authentication schemes averaged over the communication session versus α with $\sigma^2 = 0.08$ and σ^2 with $\alpha = 0.4$, respectively. Fig. 8(a) shows that the FAR

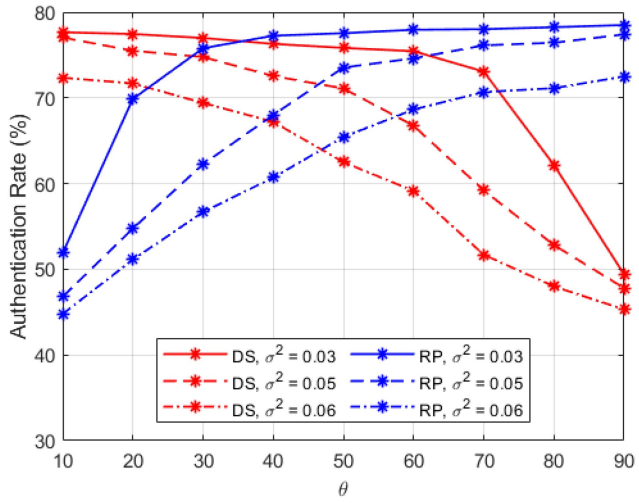

FIGURE 9. AR for the DS and RP threshold authentication schemes versus θ with $\alpha = 0.4$ and $\sigma^2 = 0.03, 0.05$, and 0.06.

for DS is lower than the FAR for RP for all values of α, and the minimum FAR is 48.9% for DS and 53.2% for RP. Fig. 8(b) indicates that the FAR for DS is lower than the FAR for RP for all values of σ^2, but there is a small increase with σ^2. For example, the FAR at $\sigma^2 = 0.02$ is 45.6% for DS and 46.3% for RP, while at $\sigma^2 = 0.09$ the AR is 48.9% for DS and 54.9% for RP. Fig. 8(a) shows that the MDR for DS is lower than the MDR for RP at low α, but at high α the converse is true. For example, the MDR with $\alpha = 0.1$ is 25.2% for DS and 35.4% for RP. On the other hand, Fig. 8(b) indicates that the MDR for DS is lower than for RP for most values of σ^2, but both increase with σ^2. For example, the MDR at $\sigma^2 = 0.03$ is 5.4% for DS and 16.2% for RP, while at $\sigma^2 = 0.08$ the corresponding values are 42.0% and 44.4%.

Figs. 8(a) and 8(b) show that the AR for DS is higher than for RP for all values of α and σ^2. For example, in Fig. 8(a) the AR at $\alpha = 0.1$ for DS is 63.1% versus 57.6% for RP. However, this difference decreases with increasing α and is less than 1% at $\alpha = 0.8$. The AR with AND is 48.4% at $\alpha = 0.1$, while for OR it is 74.5%. Both decrease with increasing α so at $\alpha = 0.9$ the AR with AND is 35.2% and with OR is 60.6%. Further, Fig. 8(b) shows that the AR for DS is higher than for RP for all values of σ^2. For example, the AR at $\sigma^2 = 0.02$ for DS is 75.5% versus 71.4% for RP. The AR with AND is 64.2% at $\sigma^2 = 0.01$ while for OR it is 88.9%. Both decrease with increasing σ^2, so at $\sigma^2 = 0.1$ the AR with AND is 36.6% and with OR is 61.3%.

Fig. 9 presents the AR for the DS and RP threshold authentication schemes versus θ with $\alpha = 0.4$ and $\sigma^2 = 0.03$, 0.05, and 0.06. This shows that the AR for DS is better than for RP at low θ, but the converse is true at high θ. For example, at $\theta = 20^\circ$ and $\sigma^2 = 0.06$, the AR for DS is 71.4% versus 51.1% for RP. However, at $\theta = 80^\circ$ and $\sigma^2 = 0.06$, the AR for DS is 48.0% versus 71.1% for RP. This shows that using DS at low θ and switching to RP at high θ can provide good authentication performance. For example, at $\sigma^2 = 0.03$, $\sigma^2 = 0.05$, and $\sigma^2 = 0.06$ the minimum AR with this approach is 76.5%, 71.6%, and 64.0%, respectively.

C. MACHINE LEARNING AUTHENTICATION SCHEME PERFORMANCE

Figs. 10(a) and 10(b) present the AR for the DS, RP, and DS and RP ML authentication schemes with $\ell = 10$ and $\eta = 0.5$ averaged over the communication session versus α with $\sigma^2 = 0.08$ and σ^2 with $\alpha = 0.4$, respectively. Fig. 10(a) shows that the AR for DS is higher than for RP for all values of α. For example, the AR at $\alpha = 0.2$ for DS is 73.3% versus 71.6% for RP, and the AR at $\alpha = 0.8$ for DS is 68.4% versus 63.1% for RP. However, the AR for DS and RP is higher than with DS or RP separately. For example, the AR at $\alpha = 0.6$ for DS and RP is 74.2% versus 71.2% for DS and 67.8% for RP. Fig. 10(b) shows that the AR for DS and RP is higher than with DS or RP separately for all values of σ^2. For example, the AR at $\sigma^2 = 0.06$ for DS and RP is 74.7% versus 74.2% for DS and 71.9% for RP.

Fig. 11 presents the AR for the separate DS and RP ML authentication schemes versus θ with $\alpha = 0.4$, $\ell = 10$, $\sigma^2 = 0.03$ and 0.06, and $\eta = 0.5$. This shows that the AR for DS is higher than for RP at low θ, but the converse is true at high θ. For example, at $\theta = 20^\circ$ and $\sigma^2 = 0.06$, the AR for DS is 74.7% versus 70.5% for RP, and at $\theta = 80^\circ$ and $\sigma^2 = 0.06$, the AR for DS is 69.0% versus 74.9% for RP. This shows that using DS at low θ and switching to RP at high θ can provide good authentication performance. For example, at $\sigma^2 = 0.03$ and $\sigma^2 = 0.06$ the minimum AR in this case is 74.3% and 74.1%, respectively.

D. AUTHENTICATION SCHEME PERFORMANCE COMPARISON

Figs. 12(a) and 12(b) present the AR for the DS, RP, AND, and OR threshold authentication schemes and the DS, RP, and DS and RP ML authentication schemes averaged over the communication session with $\eta = 0.1$ and 0.5 and $\ell = 10$ versus α with $\sigma^2 = 0.02$ and σ^2 with $\alpha = 0.3$, respectively. Fig. 12(a) shows that the AR for DS is higher than for RP for all values of α, and the AR decreases with α. Further, the AR for the DS or RP ML authentication schemes with $\eta = 0.5$ is lower than the AR for the DS or RP threshold authentication schemes at low α and higher at high α. However, the AR for DS or RP ML authentication with $\eta = 0.1$ is higher than the AR for DS or RP threshold authentication for all values of α. For example, the AR at $\alpha = 0.1$ for the DS and RP threshold authentication schemes is 76.3% and 74.7%, respectively, but the AR for the corresponding ML authentication schemes is 94.0% and 91.2% with $\eta = 0.1$ and 74.3% and 73.8% with $\eta = 0.5$, respectively. In addition, the AR at $\alpha = 0.9$ for the DS and RP threshold authentication schemes is 55.6% and 53.1%, respectively, while the AR for the corresponding ML authentication schemes is 74.9% and 66.8% with $\eta = 0.1$ and 64.3% and 60.2% with $\eta = 0.5$, respectively. However, using both DS and RP for ML authentication with $\eta = 0.1$

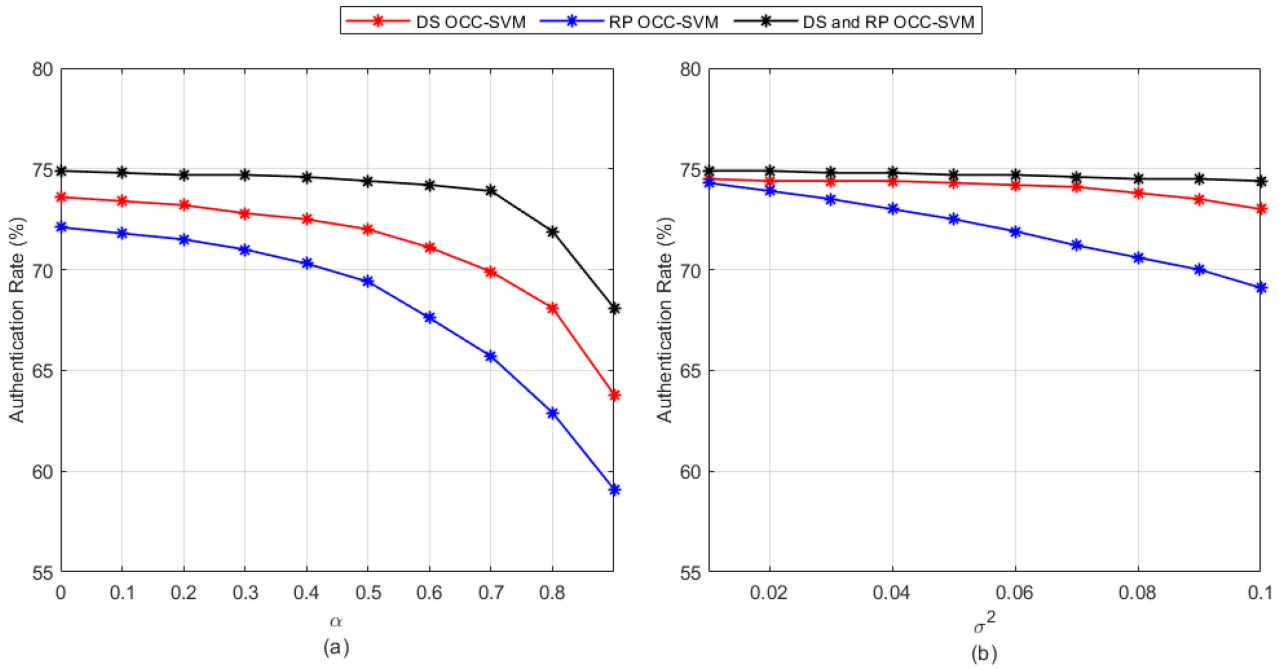

FIGURE 10. AR for the DS, RP, and DS and RP ML authentication schemes averaged over the communication session with $\eta = 0.5$ and $\ell = 10$ versus (a) α with $\sigma^2 = 0.08$, and (b) σ^2 with $\alpha = 0.4$.

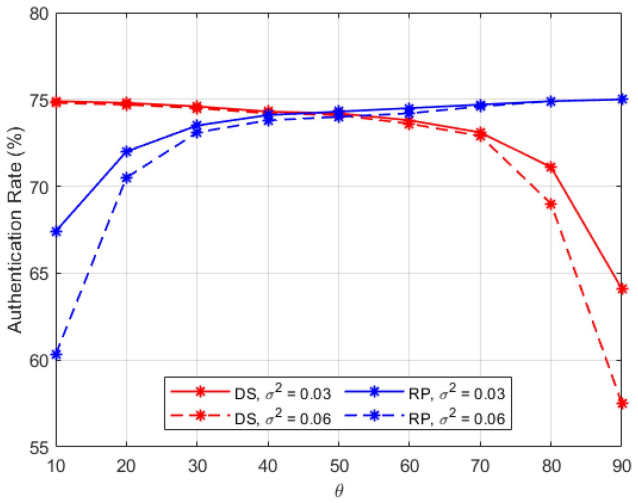

FIGURE 11. AR versus θ for the DS and RP ML authentication schemes with $\eta = 0.5$, $\alpha = 0.4$, $\ell = 10$, and $\sigma^2 = 0.03$ and 0.06.

provides the highest AR followed by OR threshold authentication, DS and RP ML authentication with $\eta = 0.5$, and then AND threshold authentication. For example, the AR at $\alpha = 0.1$ is 95.2%, 88.7%, 74.8%, and 64.0% for DS and RP ML authentication with $\eta = 0.1$, OR threshold authentication, DS and RP ML authentication with $\eta = 0.5$, and AND threshold authentication, respectively, and the corresponding AR at $\alpha = 0.8$ is 94.0%, 78.9%, 72.5%, and 53.9%, respectively.

Fig. 12(b) shows that the AR for DS or RP ML authentication with $\eta = 0.5$ is lower than the corresponding threshold authentication schemes at low σ^2 and higher at high σ^2. The AR for DS or RP ML authentication with $\eta = 0.1$ is higher than the AR for DS or RP threshold authentication for all values of σ^2. For example, the AR at $\sigma^2 = 0.01$ for DS and RP threshold authentication is 77.1% and 75.4%, respectively, but the corresponding values for ML authentication are 94.3% and 93.1% with $\eta = 0.1$ and 73.9% and 73.1% with $\eta = 0.5$, respectively. The AR at $\sigma^2 = 0.1$ for DS and RP threshold authentication is 52.0% and 49.0%, respectively. However, the AR for the ML authentication schemes with DS and RP separately is 83.4% and 71.9% with $\eta = 0.1$ and 72.0% and 67.9% with $\eta = 0.5$, respectively. The highest AR is achieved with both DS and RP ML authentication with $\eta = 0.1$. For example, the AR at $\sigma^2 = 0.01$ is 95.3%, 89.2%, 75.0%, and 64.5% for DS and RP ML authentication with $\eta = 0.1$, OR threshold authentication, DS and RP ML authentication with $\eta = 0.5$, and AND threshold authentication, respectively. Furthermore, the AR at $\sigma^2 = 0.1$ is 92.5%, 74.0%, 63.5%, and 38.1% for DS and RP ML authentication with $\eta = 0.1$, OR threshold, DS and RP ML authentication with $\eta = 0.5$, and AND threshold authentication, respectively.

Figs. 13(a) and 13(b) present the AR versus θ with $\sigma^2 = 0.04$ and $\alpha = 0.3$ for the separate DS and RP threshold and separate DS and RP ML authentication schemes with $\eta = 0.1$ and 0.5 and $\ell = 10$, and the AND threshold, OR threshold, and DS and RP ML authentication schemes with $\eta = 0.1$ and 0.5 and $\ell = 10$, respectively. Fig. 13(a) shows that the AR for DS is higher than with RP at low θ, but at high θ the AR for RP is thigher than with DS. For example, at $\theta = 20^\circ$ the AR for DS and RP threshold authentication is 77.5%

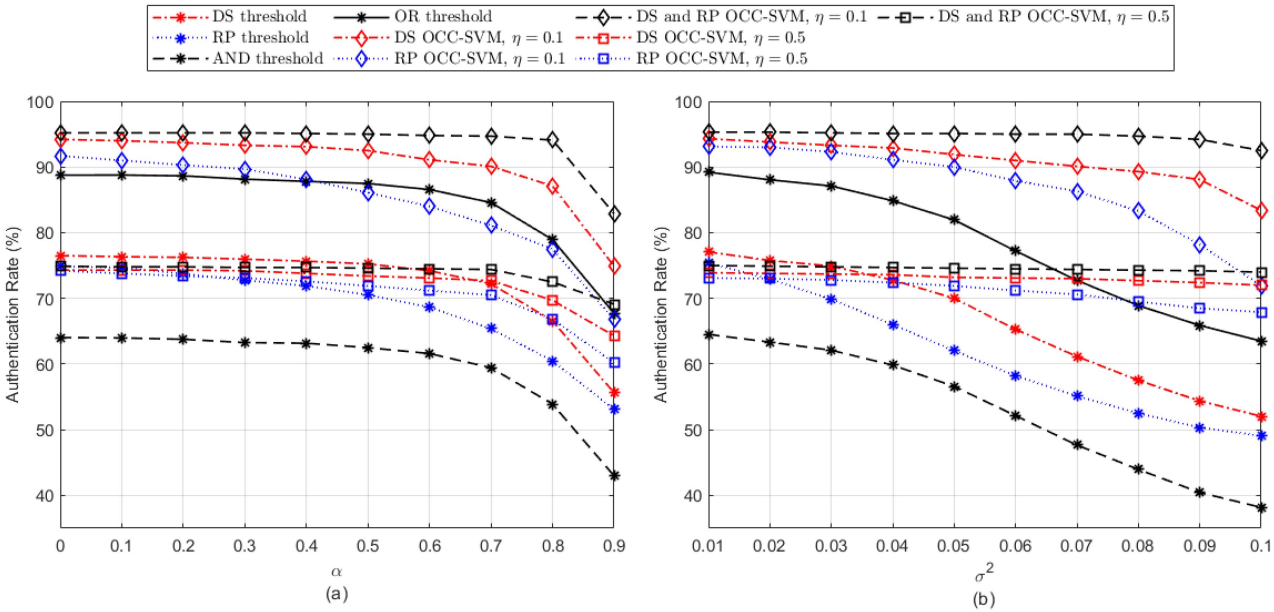

FIGURE 12. AR for the DS, RP, AND, and OR threshold authentication schemes and the DS, RP, and DS and RP ML authentication schemes averaged over the communication session with $\eta = 0.1$ and 0.5, and $\ell = 10$ versus (a) α with $\sigma^2 = 0.02$, and (b) σ^2 with $\alpha = 0.3$.

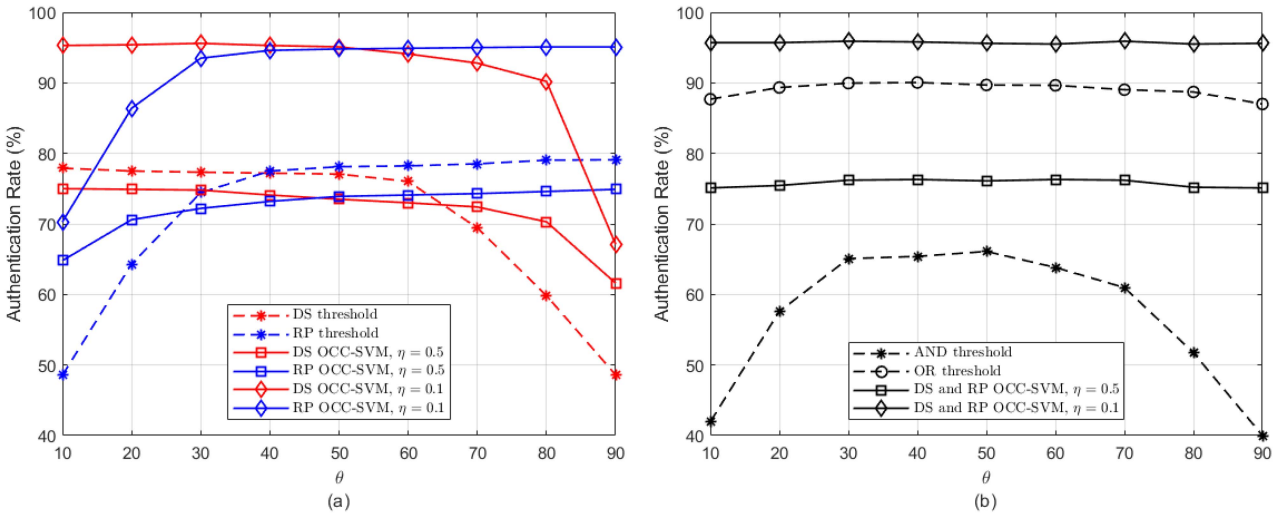

FIGURE 13. AR versus θ with $\sigma^2 = 0.04$ and $\alpha = 0.3$ for the (a) separate DS and RP threshold and separate DS and RP ML authentication schemes with $\eta = 0.1$ and 0.5 and $\ell = 10$, and (b) AND and OR threshold authentication schemes, and DS and RP ML authentication schemes with $\eta = 0.1$ and 0.5 and $\ell = 10$.

and 64.3%, respectively, and the AR for the corresponding ML authentication is 95.4% and 86.4% with $\eta = 0.1$ and 74.9% and 70.6% with $\eta = 0.5$, respectively. However, at $\theta = 80^\circ$, the AR for DS and RP threshold authentication is 59.8% and 79.0%, respectively, and the corresponding values for ML authentication are 90.2% and 95.1% with $\eta = 0.1$ and 70.3% and 74.6% with $\eta = 0.5$, respectively. Thus, it can be concluded that when the DS and RP are used separately for authentication, DS should be considered at low θ and RP at high θ. For example, in this case the minimum AR is 94.8%, 77.3%, and 73.5% for ML authentication with $\eta = 0.1$, threshold authentication, and ML authentication with $\eta = 0.5$, respectively. Finally, threshold authentication provides better performance than ML authentication with large η when DS and RP are used separately, but the converse is true with small η. Fig. 13(b) presents the AR when DS and RP are both used for authentication. This shows that with small η, ML authentication provides the highest AR. For example, at $\theta = 50^\circ$ the AR is 95.6%, 89.7%, 76.1%, and 66.1% for DS and RP ML authentication with $\eta = 0.1$, OR threshold

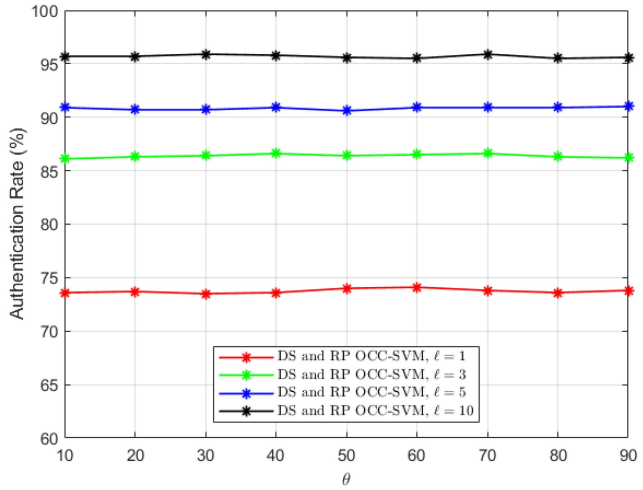

FIGURE 14. AR for DS and RP ML authentication scheme versus θ with $\sigma^2 = 0.04$, $\eta = 0.1$, and $\alpha = 0.3$ for $\ell = 1, 3, 5$ and 10.

authentication, DS and RP ML authentication with $\eta = 0.5$, and AND threshold authentication, respectively.

Fig. 14 presents the AR for DS and RP ML authentication versus θ with $\sigma^2 = 0.04$, $\eta = 0.1$, and $\alpha = 0.3$ for $\ell = 1, 3, 5$, and 10. This shows that the AR increases with ℓ. For example, at $\theta = 80^\circ$ the AR is 73.6%, 86.3%, 90.9%, and 95.5% for $\ell = 1, 3, 5$, and 10, respectively.

VI. CONCLUSION

Physical layer authentication (PLA) has emerged as an alternative paradigm that uses physical characteristics to achieve authentication. A PLA scheme was proposed for low earth orbit (LEO) satellites using Doppler frequency shift (DS) and received power (RP) characteristics. This scheme employs hypothesis testing using a threshold or machine learning (ML) to discriminate between legitimate and illegitimate satellites. Estimation errors in the DS and RP values were considered and the performance was evaluated based on real satellite data from the system tool kit (STK). Results were presented which show that DS provides a high authentication rate (AR) at small elevation angles (θ) and decreases with θ, while RP provides a low AR at small θ and increases with θ. Further, ML authentication with a small percentage of outliers η in the training data provides the highest AR. Finally, the AR for the ML authentication scheme increases with the amount of training data ℓ.

REFERENCES

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

[2] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, Jan.–Mar. 2022.

[3] 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, Oct.-Dec. 2018.

[4] 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, Apr.–Jun. 2021.

[5] 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.

[6] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "Physical layer security framework for optical non-terrestrial networks," in *Proc. Int. Conf. Telecommun.*, 2021, pp. 162–166.

[7] H. Guo, X. Zhou, J. Liu, and Y. Zhang, "Vehicular intelligence in 6G: Networking, communications, and computing," *Veh. Commun.*, vol. 33, 2022, Art. no. 100399.

[8] 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, May 2020.

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

[10] OneWeb, "OneWeb confirms successful launch of 36 satellites, After rapid year of progress," 2021. [Online]. Available: https://oneweb.net

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

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

[13] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey on threats, solutions, and research challenges," *Comput. Netw.*, vol. 216, Oct. 2022, Art. no. 109246.

[14] 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.

[15] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[16] H. Boche, R. F. Schaefer, S. Baur, and H. V. Poor, "On the algorithmic computability of the secret key and authentication capacity under channel, storage, and privacy leakage constraints," *IEEE Trans. Signal Process.*, vol. 67, no. 17, pp. 4636–4648, Sep. 2019.

[17] 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.

[18] 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.

[19] 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.

[20] 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 Navigation Symp.*, Monterey, CA, USA, Apr. 2018, pp. 1485–1491.

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

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

[23] 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, Apr. 2015, pp. 3192–3196.

[24] 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.

[25] 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.

[26] 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.
[27] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1506–1521, 2021.
[28] 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.
[29] 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.
[30] 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.
[31] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. Int. Conf. Mobile Syst., Appl., Serv.*, Washington, DC, USA, 2011, pp. 211–224.
[32] 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 Secur.*, vol. 10, no. 5, pp. 941–952, May 2015.
[33] 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.
[34] 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 Conf. Comput. Commun. Workshops*, Turin, Italy, Apr. 2013, pp. 2544–2552.
[35] 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.
[36] 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.
[37] L. Xiao, X. Lu, T. Xu, W. Zhuang, and H. Dai, "Reinforcement learning-based physical-layer authentication for controller area networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2535–2547, 2021.
[38] G. Oligeri, S. Raponi, S. Sciancalepore, and R. Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Trans. Inf. Forensics Secur.*, doi: 10.1109/TIFS.2022.3219287, 2022.
[39] 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, Oct. 2020, pp. 112–117.
[40] O. A. Topal, 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, no. 3, pp. 232–243, Sep. 2021.
[41] E. Jedermann, M. Strohmeier, M. Schäfer, J. Schmitt, and V. Lenders, "Orbit-based authentication using TDOA signatures in satellite networks," in *Proc. ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Abu Dhabi, United Arab Emirates, 2021, pp. 175–180.
[42] 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.
[43] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[44] T. Pratt and J. E. Allnutt, *Satellite Communications*. New Delhi, India: Wiley, 2020.
[45] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Computation*, vol. 13, no. 7, pp. 1443–1471, 2001.
[46] D. M. Tax and R. P. Duin, "Support vector data description," *Mach. Learn.*, vol. 54, no. 1, pp. 45–66, 2004.
[47] 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.
[48] N. Sabri, S. Aljunid, M. Salim, R. Kamaruddin, R. Ahmad, and M. Malek, "Path loss analysis of WSN wave propagation in vegetation," *J. Physics: Conf. Ser.*, vol. 423, 2013, Art. no. 012063.
[49] M. Murata, I. Kawano, and K. Inoue, "Precision onboard navigation for LEO satellite based on precise point positioning," in *Proc. IEEE/ION Position, Location Navigation Symp.*, Portland, OR, USA, Apr. 2020, pp. 1506–1513.
[50] 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. Navigation*, Portland, OR, USA, 2016, pp. 3715–3723.

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 working toward 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, information theory, security, physical layer authentication, 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, ON, Canada, 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. In 2002, he became a Fellow of the Engineering Institute of Canada and in 2012 a Fellow of the Canadian Academy of Engineering. From 2007 to 2012 he was an Editor and from 2012 to 2017 an Area Editor, of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.