RIS-aided AANETs: Security Maximization Relying on Unsupervised Projection-based Neural Networks

Tiep M. Hoang, Thien Van Luong, Dong Liu, and Lajos Hanzo

***Abstract*—The security aspects of aeronautical *ad-hoc* networks (AANET) relying on reflective intelligent surface (RIS) are considered. A projection-based deep neural network (DNN) is designed for maximizing the secrecy rate of the proposed RIS-aided AANET. While the multiple-layer architecture of the DNN enables learning the functional relationship between the target variables of the optimization problem and the ground-air channels, the projection method guarantees that the constraint of the optimization problem is not violated. Our design outperforms the state-of-the-art projected gradient descent algorithms and that the RIS is capable of enhancing the security.**

***Index terms*—**Physical layer security, reliability, deep learning, projection neural network.

I. Introduction

The concept of aeronautical *ad-hoc* networks (AANET) has been developed with the objective of allowing aircraft to assist information exchange in 6G [1]. In this vein, AANETs are expected to combine spaceborne and terrestrial networks to improve the global connectivity in remote areas. One of the challenges to be faced by AANETs is the maintenance of stable connection with aeroplanes that move at high speeds and hence experience both link delays and grave Doppler effects. Additionally, like other wireless networks, an AANET faces potential information leakage to eavesdroppers due to the broadcast nature of wireless propagation. Thus, the physical layer security (PLS) of an AANET has also been examined as one of the important aspects [2]. However, there is still a paucity of investigations into this salient topic. In parallel with AANETs, reflective intelligent surfaces (RISs) have also been developed for high-integrity transmissions. An RIS may act as a *passive* relay, because it does not have to amplify (or detect/decode) its received signal, as in classic amplify-and-forward or decode-and-forward relaying. Inspired by this, RIS-assisted PLS has been touched upon in [3]–[6], but it is still in its infancy.

Nijsure *et al.* [2] developed a geolocation mechanism to estimate the location of aircraft in support of reliable and secure air-to-ground communication links. However, no RISs and security optimization were considered in [2]. On the other hand, the authors of [3] and [4] considered the PLS of RIS-aided terrestrial systems and used conventional iterative algorithms for solving their security maximization problem. The algorithm proposed in [3], as well as that in [4], requires multiple sub-algorithms to deal with the optimization of individual variables. At the same time, the authors of [5] investigated the security of an RIS-aided terrestrial communication system and optimized the secrecy rate using reinforcement learning. In [7] and [8], the beamforming and the phase shifts of RISs are jointly optimized for enhancing the security. Furthermore, Song *et al.* [6] investigated a similar system but used supervised learning for optimizing the secrecy rate. From an experimental perspective, the loss function of the supervised neural network of [6] depends heavily on the availability of built-in functions of the `tensorflow` framework; thus, it cannot be readily extended to any other loss functions. Another drawback of [6] is the requirement of specific target values for the comparison of the values found by the supervised learning algorithm. In contrast to [5], we consider unsupervised learning, which has the advantage of not requiring rewards and punishments through the interaction with the environment. Additionally, in contrast to [6], our approach does not require the availability of target values and reflects a more flexible approach, because the objective function of our optimization problem can be readily converted into the loss function of an unsupervised neural network. Moreover, the focus of our work is on the PLS of AANETs characterized by extremely high Doppler effects, rather than on the security of terrestrial networks. Our bold and explicit novelty statement is contrasted to the literature in Table I, which is detailed on the next page.

Again, the PLS solutions considered in [3]–[8] were not dedicated to AANETs, while the PLS-aided AANETs of [2] did not consider the benefits of RISs. We will thus investigate the PLS of an RIS-aided AANET, given that AANETs can play a pivotal role in 6G and RISs have the potential of reconfiguring the propagation environment to protect against eavesdropping. Moreover, we also aim to find a joint beamforming and RIS design for maximizing the average secrecy rate of our proposed system. To deal with the proposed optimization problem, we design a so-called *projection*-based deep neural network (DNN), which will output suitable solutions. Note that joint optimization problems are also considered in [7] and [8], but no DNN solutions are proposed. Harnessing the power of deep learning (DL), our projection-based DNN is constituted by an intrinsic analysis of the DNN and of the projection method [9]. While the the DNN solves the proposed opti-

T. M. Hoang and L. Hanzo are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK (e-mails: {tiep.hoang, lh}@soton.ac.uk).

T. V. Luong was with University of Southampton, UK. He is now with the Faculty of Computer Science, Phenikaa University, Hanoi 12116, Vietnam (e-mail: thien.luongvan@phenikaa-uni.edu.vn).

D. Liu is with the School of Cyber Science and Technology, Beihang University, Beijing 100191, China (email: dliu@buaa.edu.cn).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028).

TABLE I: Contrasting our contribution to the literature

	[2] - 2015	[3] - 2019	[4] - 2019	[5] - 2020	[6] - 2020	[7] - 2020	[8] - 2020	This work
RIS-assisted security		✓	✓	✓	✓	✓	✓	✓
Security for AANETs	✓							✓
Unsupervised learning								✓
Reinforcement learning				✓				
Projection methods								✓
Joint reflecting and precoding design		✓	✓	✓		✓	✓	✓
Rician fading	✓		✓		✓			✓
Temporal/spatial correlation			✓	✓	✓			✓

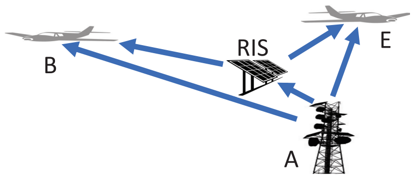

Fig. 1: System model.

mization problem without constraints, the projection method guarantees that the output of the DNN will then be projected onto the constraint domain. To demonstrate the efficiency of our projection-based DNN, we compare it with two different conventional techniques, i.e. the projected gradient descent (PGD) and Nesterov's PGD [10]. Our proposed technique is shown to outperform a pair of PGD approaches. Moreover, our results show that a useful positive secrecy rate can be attained under diverse circumstances.

The remainder of the paper is organized as follows. Section II presents both the system model and the channel model of the RIS-aided AANET. Section III formulates the security maximization problem and also presents the proposed projection-based DNN in detail. Section IV provides our numerical results and finally, Section V provides the conclusions of the paper.

Notations: $\mathbb{C}^{m\times n}$ denotes the complex field that includes all complex-valued matrices of size $m \times n$; The operation $\text{diag}\left([z_1,\ldots,z_K]\right)$ diagonalizes a row vector $[z_1,\ldots,z_K]$ into a diagonal matrix; $\mathbf{I}_n$ denotes the identity matrix of size $n \times n$; The upperscripts $(\cdot)^\top$, $(\cdot)^*$, and $(\cdot)^\dagger$ represent the transpose, conjugate, and Hermitian operators, respectively; $\mathbf{z} \sim \mathcal{CN}\left(\mathbf{m},\mathbf{\Sigma}\right)$ is a complex Gaussian random vector with mean $\mathbf{m}$ and covariance matrix $\mathbf{\Sigma}$; $\nabla_{\mathbf{z}} f(\mathbf{z})$ denotes the gradient of $f(\mathbf{z})$ with respect to $\mathbf{z}$; $\nabla_{\mathbf{z}} f(\mathbf{z})\big|_{\mathbf{z}=\mathbf{z}_0}$ represents the gradient of $f(\mathbf{z})$ evaluated at $\mathbf{z}=\mathbf{z}_0$.

II. System Model and Channel Modelling

A. System Model

We consider an AANET, which operates in the super-high-frequency (SHF) band spanning (from 3 GHz to 30 GHz). Moreover, the AANET relies on a reconfigurable intelligent surface (denoted by R) of multiple reflecting elements placed near the ground station in order to assist the transmission. In this RIS-aided AANET, a ground station (denoted by A) communicates with a legitimate aircraft (denoted by B) in the presence of an unintended eavesdropping aircraft (E). While B and E are assumed to be moving aircraft, A and R are static objects on the ground. Moreover, R is near A to assist the transmission. We assume that A is equipped with $N_{\mathtt{A}}$ antennas, while both B and E have a single SHF antenna.[1] Due to the broadcast of wireless transmission, both B and E receive confidential messages from A, even though A only wants to convey its confidential messages to B. Since a fraction of the local oscillator signal can leak out from the local oscillator of E [12], A is supposed to have the statistical knowledge of the estimated eavesdropping channels.

1) The signals received at B and E: The signal received at B, with the aid of the RIS, can be given by

$$z_{\mathtt{B}} = \left(10^{-\frac{\mathfrak{L}_{\mathtt{ARB}}}{20}}\mathbf{h}_{\mathtt{RB}}\mathbf{\Psi}_{\mathtt{R}}\mathbf{H}_{\mathtt{AR}} + 10^{-\frac{\mathfrak{L}_{\mathtt{AB}}}{20}}\mathbf{h}_{\mathtt{AB}}\right)\mathbf{f}^\top s_{\mathtt{A}} + n_{\mathtt{B}}, \quad (1)$$

$\mathfrak{L}_{\mathtt{AB}}$ is the path loss (in dB) of the direct $\mathtt{A}\to\mathtt{B}$ link; $\mathfrak{L}_{\mathtt{ARB}}$ is the effective path loss (in dB) of the $\mathtt{A}\to\mathtt{R}\to\mathtt{B}$ link; $\mathbf{H}_{\mathtt{AR}} \in \mathbb{C}^{K_{\mathtt{R}}\times N_{\mathtt{A}}}$ is the small-scale channel fading for the $\mathtt{A}\to\mathtt{R}$ link; $\mathbf{h}_{\mathtt{RB}} \in \mathbb{C}^{1\times K_{\mathtt{R}}}$ is the small-scale channel fading for the $\mathtt{R}\to\mathtt{B}$ link; $\mathbf{h}_{\mathtt{AB}} \in \mathbb{C}^{1\times N_{\mathtt{A}}}$ is the small-scale channel fading for the $\mathtt{A}\to\mathtt{B}$ link; $\mathbf{\Psi}_{\mathtt{R}} = \text{diag}\left(\left[e^{j2\pi\psi_1},\ldots,e^{j2\pi\psi_{K_{\mathtt{R}}}}\right]\right) \in \mathbb{C}^{K_{\mathtt{R}}\times K_{\mathtt{R}}}$ is the diagonal matrix that reflects the phase-shift caused by the RIS; $\mathbf{f} \in \mathbb{C}^{1\times N_{\mathtt{A}}}$ is the beamforming vector; $s_{\mathtt{A}}$ is the original signal with the average power $\mathbb{E}\left\{|s_{\mathtt{A}}|^2\right\} = P_{\mathtt{A}}$ in Watt (W); $n_{\mathtt{B}}$ is the additive white Gaussian noise (AWGN) at B, which obeys the complex Gaussian distribution with zero-mean and noise variance N_0, i.e., $n_{\mathtt{B}} \sim \mathcal{CN}\left(0, N_0\right)$. To ensure that the transmit power is less than or equal to $P_{\mathtt{A}}$, we have the constraint $\|\mathbf{f}\|^2 \le 1$.

Similarly, the signal received at E is given by

$$z_{\mathtt{E}} = \left(10^{-\frac{\mathfrak{L}_{\mathtt{ARE}}}{20}}\mathbf{h}_{\mathtt{RE}}\mathbf{\Psi}_{\mathtt{R}}\mathbf{H}_{\mathtt{AR}} + 10^{-\frac{\mathfrak{L}_{\mathtt{AE}}}{20}}\mathbf{h}_{\mathtt{AE}}\right)\mathbf{f}^\top s_{\mathtt{A}} + n_{\mathtt{E}}, \quad (2)$$

where $\mathfrak{L}_{\mathtt{AE}}$ is the path loss (in dB) of the direct $\mathtt{A}\to\mathtt{E}$ link; $\mathfrak{L}_{\mathtt{ARE}}$ is the effective path loss (in dB) of the $\mathtt{A}\to\mathtt{R}\to\mathtt{E}$ link; $\mathbf{h}_{\mathtt{RE}} \in \mathbb{C}^{1\times K_{\mathtt{R}}}$ is the channel of the $\mathtt{R}\to\mathtt{E}$ link, $\mathbf{h}_{\mathtt{AE}} \in \mathbb{C}^{1\times N_{\mathtt{A}}}$ is the channel of the $\mathtt{A}\to\mathtt{E}$ direct link, $n_{\mathtt{E}}$ is the AWGN at E with $n_{\mathtt{E}} \sim \mathcal{CN}\left(0,1\right)$.

B. Channel Modelling

Due to the short distance between A and R, we assume that there are blockages around them, which wipe out the line-of-sight component. Each entry in $\mathbf{H}_{\mathtt{AR}}$ is thus assumed to obey an independent complex Gaussian distribution with zero-mean and unit variance. However, for the channels $\mathbf{h}_{\mathtt{RB}}, \mathbf{h}_{\mathtt{AB}}, \mathbf{h}_{\mathtt{RE}}, \mathbf{h}_{\mathtt{AE}}$, we assume that they are Rician fading channels having both line-of-sight (LoS) and non-line-of-sight

[1] In addition to the SHF antenna, an aircraft is also equipped with other types of antennas (e.g., the HF, VHF, UHF and SatCom antennas) each having a specific purpose [11].

(NLoS) components. To be more precise, a channel $\mathbf{h}_{ij}$, with $i \in \{\mathtt{A}, \mathtt{R}\}$ and $j \in \{\mathtt{B}, \mathtt{E}\}$, can be modelled as follows [13]:

$$\mathbf{h}_{ij} = \sqrt{\kappa/(\kappa+1)}\ \mathbf{h}_{ij}^{\mathrm{L}} + \sqrt{1/(\kappa+1)}\ \mathbf{h}_{ij}^{\mathrm{N}}, \tag{3}$$

where κ is the Rician factor, $\{\cdot\}_{ij}^{\mathrm{L}}$ denotes the deterministic LoS component, and $\{\cdot\}_{ij}^{\mathrm{N}}$ denotes the scattered NLoS channel component. Since both $\mathtt{B}$ and $\mathtt{E}$ represent aircraft moving at a high speed, we have to consider the Doppler effect. To capture this phenomenon analytically, we use the first order stationary Gauss-Markov process to describe the *temporal* correlation between the realization of $\mathbf{h}_{ij}^{\mathrm{N}}$ at the t-th time slot, namely $\mathbf{h}_{ij}^{\mathrm{N}}[t]$, and the realization of $\mathbf{h}_{ij}^{\mathrm{N}}$ at the $(t+1)$-th time slot, namely $\mathbf{h}_{ij}[t+1]^{\mathrm{N}}$. According to [14], we have

$$\begin{cases} \mathbf{h}_{ij}^{\mathrm{N}}[0] = \widetilde{\mathbf{h}_{ij}^{\mathrm{N}}}[0], \\ \mathbf{h}_{ij}^{\mathrm{N}}[1] = \tau_j\ \mathbf{h}_{ij}^{\mathrm{N}}[0] + \sqrt{1-\tau_j^2}\ \widetilde{\mathbf{h}_{ij}^{\mathrm{N}}}[1], \\ \dots \\ \mathbf{h}_{ij}^{\mathrm{N}}[t+1] = \tau_j\ \mathbf{h}_{ij}^{\mathrm{N}}[t] + \sqrt{1-\tau_j^2}\ \widetilde{\mathbf{h}_{ij}^{\mathrm{N}}}[t+1], \end{cases} \tag{4}$$

where τ_j is the *temporal* correlation coefficient associated with the high mobility of the object of interest $j \in \{\mathtt{B}, \mathtt{E}\}$. Note that each element in $\widetilde{\mathbf{h}_{ij}^{\mathrm{N}}}[0]$, as well as each element in $\widetilde{\mathbf{h}_{ij}^{\mathrm{N}}}[t+1]$, obeys $\mathcal{CN}(0,1)$. Furthermore, τ_j is described by the Jakes model (see [14]) as $\tau_{\mathtt{B}} = J_0(2\pi f_{\mathrm{D},j} \varUpsilon_{\text{symbol}})$, where $J_0(\cdot)$ is the zeroth-order Bessel functions of the first kind [15, eq. (8.402)], $\varUpsilon_{\text{symbol}}$ is the transmit symbol interval, and f_{D} is the maximum Doppler frequency shift for $j \in \{\mathtt{B}, \mathtt{E}\}$. Note that the product $f_{\mathrm{D},j}\varUpsilon_{\text{symbol}} \triangleq \overline{f}_{\mathrm{D},j}$ is the maximum *normalized* Doppler shift [16], [17]. To model $\overline{f}_{\mathrm{D},j}$, we will use $\overline{f}_{\mathrm{D},j} = f_{\mathrm{D},j}\varUpsilon_{\text{symbol}} = (v_j f_c/c) \times (1/f_{\text{Baud}})$, where v_j [m/s] is the velocity of $j \in \{\mathtt{B}, \mathtt{E}\}$; $c = 3 \times 10^8$ [m/s] is the speed of light; and f_{Baud} is the Baud rate of the L-DACS1 of the *L-band digital aeronautical communication system* (L-DACS), which is a potential framework for the future AANET, where f_{Baud} can be chosen to be 625 kHz.

III. Security Maximization Relying on Unsupervised Learning

We can deduce from (1) and (2) that the instantaneous SNRs received at $\mathtt{B}$ and $\mathtt{E}$ are as follows:

$$\varGamma_{\mathtt{B}} = P_{\mathtt{A}} \left\| \left(\beta_{\mathtt{ARB}} \mathbf{h}_{\mathtt{RB}} \varPsi_{\mathtt{R}} \mathbf{H}_{\mathtt{AR}} + \beta_{\mathtt{AB}} \mathbf{h}_{\mathtt{AB}} \right) \mathbf{f}^{\top} \right\|^2, \tag{5}$$

$$\varGamma_{\mathtt{E}} = P_{\mathtt{A}} \left\| \left(\beta_{\mathtt{ARE}} \mathbf{h}_{\mathtt{RE}} \varPsi_{\mathtt{R}} \mathbf{H}_{\mathtt{AR}} + \beta_{\mathtt{AE}} \mathbf{h}_{\mathtt{AE}} \right) \mathbf{f}^{\top} \right\|^2, \tag{6}$$

where $\beta_{\mathtt{ARB}} = \sqrt{\frac{10^{-(\mathfrak{L}_{\mathtt{ARB}}/10)}}{N_0}}$, $\beta_{\mathtt{ARE}} = \sqrt{\frac{10^{-(\mathfrak{L}_{\mathtt{ARE}}/10)}}{N_0}}$, $\beta_{\mathtt{AB}} = \sqrt{\frac{10^{-(\mathfrak{L}_{\mathtt{AB}}/10)}}{N_0}}$ and $\beta_{\mathtt{AE}} = \sqrt{\frac{10^{-(\mathfrak{L}_{\mathtt{AE}}/10)}}{N_0}}$. From a practical perspective, we assume that $\mathbf{h}_{\mathtt{AE}}$ and $\mathbf{h}_{\mathtt{RE}}$ are not available; instead, we only have imperfect channel state information for $\mathtt{E}$. Let $\mathbf{h}_{\mathtt{AE}}^{\text{est}}$ and $\mathbf{h}_{\mathtt{RE}}^{\text{est}}$ be the estimate of $\mathbf{h}_{\mathtt{AE}}$ and that of $\mathbf{h}_{\mathtt{RE}}$, respectively. According to [18], the relationship between $\mathbf{h}_{\mathtt{AE}}^{\text{est}}$ and $\mathbf{h}_{\mathtt{AE}}$ can be modelled as $\mathbf{h}_{\mathtt{AE}} = \sqrt{1-\zeta^2}\ \mathbf{h}_{\mathtt{AE}}^{\text{est}} + \zeta\ \mathbf{e}_{\mathtt{AE}}$, where $\mathbf{e}_{\mathtt{AE}} \sim \mathcal{CN}(0,1)$ is the channel estimation error, and $\zeta \in (0,1)$ denotes the estimation error coefficient. Similarly, we have $\mathbf{h}_{\mathtt{RE}} = \sqrt{1-\zeta^2}\ \mathbf{h}_{\mathtt{RE}}^{\text{est}} + \zeta\ \mathbf{e}_{\mathtt{RE}}$, where $\mathbf{e}_{\mathtt{RE}} \sim \mathcal{CN}(0,1)$.

Let $\varGamma_{\mathtt{E}}^{\text{est}}$ be the instantaneous estimated SNR at $\mathtt{E}$, known to the operators, which can be readily calculated upon replacing $\{\mathbf{h}_{\mathtt{AE}}, \mathbf{h}_{\mathtt{RE}}\}$ in (6) by $\{\mathbf{h}_{\mathtt{AE}}^{\text{est}}, \mathbf{h}_{\mathtt{RE}}^{\text{est}}\}$, i.e.,

$$\varGamma_{\mathtt{E}}^{\text{est}} = P_{\mathtt{A}} \left\| \left(\beta_{\mathtt{ARE}} \mathbf{h}_{\mathtt{RE}}^{\text{est}} \varPsi_{\mathtt{R}} \mathbf{H}_{\mathtt{AR}} + \beta_{\mathtt{AE}} \mathbf{h}_{\mathtt{AE}}^{\text{est}} \right) \mathbf{f}^{\top} \right\|^2. \tag{7}$$

Then, relying on (5) and (7), we will be able to quantify the *instantaneous* secrecy rate at the t-th time slot as $C_s\left(\boldsymbol{\psi}, \mathbf{f} \left| \mathcal{S}_{\text{est}}^{[t]} \right.\right) = \max\left(0, \log_2\left(\frac{1+\varGamma_{\mathtt{B}}}{1+\varGamma_{\mathtt{E}}^{\text{est}}}\right)\right)$, where $\boldsymbol{\psi} = [\psi_1, \dots, \psi_{K_{\mathtt{R}}}]$, and $\mathcal{S}_{\text{est}}^{[t]}$ is the channel observations at the t-th time slot, i.e.,

$$\mathcal{S}_{\text{est}}^{[t]} \triangleq \{\mathbf{H}_{\mathtt{AR}}[t], \mathbf{h}_{\mathtt{RB}}[t], \mathbf{h}_{\mathtt{AB}}[t], \mathbf{h}_{\mathtt{RE}}^{\text{est}}[t], \mathbf{h}_{\mathtt{AE}}^{\text{est}}[t]\}. \tag{8}$$

The relationship between $\boldsymbol{\psi}$ and $\varPsi_{\mathtt{R}}$ can be expressed as $\varPsi_{\mathtt{R}} = \mathsf{diag}\left(e^{j2\pi\boldsymbol{\psi}}\right)$, where $e^{j2\pi\boldsymbol{\psi}} \triangleq \left[e^{j2\pi\psi_1}, \dots, e^{j2\pi\psi_{K_{\mathtt{R}}}}\right]$. Finally, the average secrecy rate can be calculated as

$$\overline{C_s}(\boldsymbol{\psi}, \mathbf{f}) = \frac{1}{B}\sum_{t=1}^{B} C_s\left(\boldsymbol{\psi}, \mathbf{f} \left| \mathcal{S}_{\text{est}}^{[t]} \right.\right), \tag{9}$$

over a batch of B samples.[2]

A. Security Maximization

Our goal is to find the functional relationship between the channels and $(\boldsymbol{\psi}, \mathbf{f})$ so that $\overline{C_s}(\boldsymbol{\psi}, \mathbf{f})$ is maximized. Thus, the proposed optimization problem can be expressed as follows:

$$\text{Given a batch} \quad \mathcal{B} = \left\{\mathcal{S}_{\text{est}}^{[1]}, \dots, \mathcal{S}_{\text{est}}^{[B]}\right\}, \tag{10a}$$

$$\underset{\boldsymbol{\psi}=\{\psi_k\}_{k=1}^{K_{\mathtt{R}}}, \mathbf{f}}{\text{maximize}} \quad \frac{1}{B}\sum_{t=1}^{B} C_s\left(\boldsymbol{\psi}, \mathbf{f} \left| \mathcal{S}_{\text{est}}^{[t]} \right.\right), \tag{10b}$$

$$\text{subject to} \quad \|\mathbf{f}\|^2 \leq 1 \text{ and } 0 \leq \psi_k \leq 1. \tag{10c}$$

Recall that the first constraint originates from the maximum normalized transmit power $\mathbb{E}\left\{\|\mathbf{f}s_{\mathtt{A}}\|^2\right\} \leq 1$, given that $\mathbb{E}\left\{|s_{\mathtt{A}}|^2\right\} = 1$. By contrast, the second constraint is related to the reflecting elements of the RIS.

B. Deep Learning-aided Approach

In general, the constrained optimization problem (10) is non-convex and difficult to be solved analytically. In other words, it is an open challenge to find the closed-form expression for $\boldsymbol{\psi}$ and $\mathbf{f}$, even when the distribution of the channels are know. In this work, we first parametrize the elements of $\boldsymbol{\psi}$ and $\mathbf{f}$ as the functions to be optimized, we will then propose an unsupervised DL-aided approach for tackling this problem. In particular, we do not rely on a prior knowledge of the channels, but rather on the *observed/measured* values of the channels to find suitable values of $\boldsymbol{\psi}$ and $\mathbf{f}$.[3]

Prior to describing our DL-aided approach in detail, we first provide Table II capturing our notations at a glance. Based on the definitions in Table II, we have the following facts:

[2] To calculate the actual average secrecy rate, we replace $\mathcal{S}_{\text{est}}^{[t]}$ in (9) by $\mathcal{S}^{[t]}$.

[3] Our problem can also be extended to the case of multiple antennas at $\mathtt{B}$ and/or $\mathtt{E}$, as investigated in [19]. In such a case, the vector $\mathbf{f}$ will be replaced by some matrix $\mathbf{F}$ and the goal will be to optimize the column/row vectors of $\mathbf{F}$. To this effect, we can replicate the process of finding $\mathbf{f}$ and harness more output neurons. However, we leave this direction for future research.

TABLE II: A list of main notations associated with the RIS and the DNN.

Parameters	Definitions
$\boldsymbol{\theta}$	the vector capturing all the weights and biases of a DNN
$\boldsymbol{\psi}_{\boldsymbol{\theta}}$	$\boldsymbol{\psi}_{\boldsymbol{\theta}} = \left[\psi_{\boldsymbol{\theta},1}, \ldots, \psi_{\boldsymbol{\theta},K_{\mathtt{R}}}\right]$, where each element is a *real-valued* function parameterized by $\boldsymbol{\theta}$
$\mathbf{f}_{\boldsymbol{\theta}}$	$\mathbf{f}_{\boldsymbol{\theta}} = \left[f_{\boldsymbol{\theta},1}, \ldots, f_{\boldsymbol{\theta},N_{\mathtt{A}}}\right]$, where each element is a *complex-valued* function parameterized by $\boldsymbol{\theta}$
$\widehat{\mathbf{f}}_{\boldsymbol{\theta}}$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta}}$	$\widehat{\mathbf{f}}_{\boldsymbol{\theta}} = \left[\Re\left\{f_{\boldsymbol{\theta},1}\right\}, \ldots, \Re\left\{f_{\boldsymbol{\theta},N_{\mathtt{A}}}\right\}\right]$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta}} = \left[\Im\left\{f_{\boldsymbol{\theta},1}\right\}, \ldots, \Im\left\{f_{\boldsymbol{\theta},N_{\mathtt{A}}}\right\}\right]$
$\{\cdot\}^{[t,\epsilon]}$	the indicator of the t-th sample and the ϵ-th epoch
$\psi_k^{[t,\epsilon]}$	the observed value of the k-th element $\psi_{\boldsymbol{\theta},k}$ in $\boldsymbol{\psi}_{\boldsymbol{\theta}}$ at the ϵ-th epoch, w.r.t. the sample $\mathcal{S}_{\text{est}}^{[t]}$
$f_n^{[t,\epsilon]}$	the observed value of the n-th element $f_{\boldsymbol{\theta},n}$ in $\mathbf{f}_{\boldsymbol{\theta}}$ at the ϵ-th epoch, w.r.t. the sample $\mathcal{S}_{\text{est}}^{[t]}$
$\widehat{f}_n^{[t,\epsilon]}$ and $\widetilde{f}_n^{[t,\epsilon]}$	$\widehat{f}_n^{[t,\epsilon]} = \Re\left\{f_n^{[t,\epsilon]}\right\}$ and $\widetilde{f}_n^{[t,\epsilon]} = \Im\left\{f_n^{[t,\epsilon]}\right\}$
$\widehat{\mathbf{f}}^{[t,\epsilon]}$ and $\widetilde{\mathbf{f}}^{[t,\epsilon]}$	$\widehat{\mathbf{f}}^{[t,\epsilon]} = \left[\widehat{f}_1^{[t,\epsilon]}, \ldots, \widehat{f}_{N_{\mathtt{A}}}^{[t,\epsilon]}\right]$ and $\widetilde{\mathbf{f}}^{[t,\epsilon]} = \left[\widetilde{f}_1^{[t,\epsilon]}, \ldots, \widetilde{f}_{N_{\mathtt{A}}}^{[t,\epsilon]}\right]$ are the realizations of $\widehat{\mathbf{f}}_{\boldsymbol{\theta}}$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta}}$ at the ϵ-th epoch, w.r.t. the sample $\mathcal{S}_{\text{est}}^{[t]}$
$\psi_n^{[t,\epsilon]}$	the observed value of the k-th element in $\boldsymbol{\psi}_{\boldsymbol{\theta}}$ at the ϵ-th epoch, w.r.t. the sample $\mathcal{S}_{\text{est}}^{[t]}$
$\boldsymbol{\psi}^{[t,\epsilon]}$	the observed value of $\boldsymbol{\psi}_{\boldsymbol{\theta}}$ at the ϵ-th epoch, w.r.t. the sample $\mathcal{S}_{\text{est}}^{[t]}$

- The DNN is trained over multiple epochs to improve performance. At epoch ϵ, we have $\widehat{\mathbf{f}}^{[t,\epsilon]}$, $\widetilde{\mathbf{f}}^{[t,\epsilon]}$ and $\boldsymbol{\psi}^{[t,\epsilon]}$ when passing $\mathcal{S}_{\text{est}}^{[t]}$ through the DNN.
- Upon convergence, i.e., when ϵ is high enough, we consider $\mathbf{f}^{[t,\epsilon]}$ and $\boldsymbol{\psi}^{[t,\epsilon]}$ as the *desired* values corresponding to the t-th sample $\mathcal{S}_{\text{est}}^{[t]}$ upon passing the batch $\mathcal{B} = \left\{\mathcal{S}_{\text{est}}^{[t]}\right\}_{t=1}^{B}$, we will obtain $\left\{\mathbf{f}^{[1,\epsilon]}, \ldots, \mathbf{f}^{[B,\epsilon]}\right\}$ and $\left\{\boldsymbol{\psi}^{[1,\epsilon]}, \ldots, \boldsymbol{\psi}^{[B,\epsilon]}\right\}$ as the desired values.
- The functional relationship between the sample $\mathcal{S}_{\text{est}}^{[t]}$ and the value $\boldsymbol{\psi}^{[t,\epsilon]}$ is then described as follows:

$$\begin{aligned} &\boldsymbol{\psi}^{[t,\epsilon]} \triangleq \left[\psi_1^{[t,\epsilon]}, \ldots, \psi_{K_{\mathtt{R}}}^{[t,\epsilon]}\right] \\ &\quad \| \\ &\boldsymbol{\psi}_{\boldsymbol{\theta}}\left(\mathcal{S}_{\text{est}}^{[t]}\right) \triangleq \left[\psi_{\boldsymbol{\theta},1}\left(\mathcal{S}_{\text{est}}^{[t]}\right), \ldots, \psi_{\boldsymbol{\theta},K_{\mathtt{R}}}\left(\mathcal{S}_{\text{est}}^{[t]}\right)\right]. \end{aligned} \tag{11}$$

  The above relationship can be further simplified by the mapping $\psi_{\boldsymbol{\theta},k} : \mathcal{S}_{\text{est}}^{[t]} \rightarrow \psi_k^{[t,\epsilon]}$. Note that the mapping $\psi_{\boldsymbol{\theta},k}$ is a parameterized function, which is found by the DNN by the process of learning the samples $\{\mathcal{S}_{\text{est}}^{[t]}\}_{t=1}^{B}$.
- The functional relationship between the sample $\mathcal{S}_{\text{est}}^{[t]}$ and the value $\mathbf{f}^{[t,\epsilon]}$ can be described as follows:

$$\begin{aligned} &\mathbf{f}^{[t,\epsilon]} \triangleq \overbrace{\left[\widehat{f}_1^{[t,\epsilon]}, \ldots, \widehat{f}_{N_{\mathtt{A}}}^{[t,\epsilon]}\right]}^{=\,\widehat{\mathbf{f}}^{[t,\epsilon]}} + j \times \overbrace{\left[\widetilde{f}_1^{[t,\epsilon]}, \ldots, \widetilde{f}_{N_{\mathtt{A}}}^{[t,\epsilon]}\right]}^{=\,\widetilde{\mathbf{f}}^{[t,\epsilon]}} \\ &\| \\ &\mathbf{f}_{\boldsymbol{\theta}}\left(\mathcal{S}_{\text{est}}^{[t]}\right) \triangleq \underbrace{\left[\widehat{f}_{\boldsymbol{\theta},1}\left(\mathcal{S}_{\text{est}}^{[t]}\right), \ldots, \widehat{f}_{\boldsymbol{\theta},N_{\mathtt{A}}}\left(\mathcal{S}_{\text{est}}^{[t]}\right)\right]}_{=\,\widehat{\mathbf{f}}_{\boldsymbol{\theta}}\left(\mathcal{S}_{\text{est}}^{[t]}\right)} \\ &\qquad + \; j \times \underbrace{\left[\widetilde{f}_{\boldsymbol{\theta},1}\left(\mathcal{S}_{\text{est}}^{[t]}\right), \ldots, \widetilde{f}_{\boldsymbol{\theta},N_{\mathtt{A}}}\left(\mathcal{S}_{\text{est}}^{[t]}\right)\right]}_{=\,\widetilde{\mathbf{f}}_{\boldsymbol{\theta}}\left(\mathcal{S}_{\text{est}}^{[t]}\right)}. \end{aligned} \tag{12}$$

  The above relationship can be further simplified by the mappings $\widehat{f}_{\boldsymbol{\theta},n} : \mathcal{S}_{\text{est}}^{[t]} \rightarrow \widehat{f}_n^{[t,\epsilon]}$ and $\widetilde{f}_{\boldsymbol{\theta},n} : \mathcal{S}_{\text{est}}^{[t]} \rightarrow \widetilde{f}_n^{[t,\epsilon]}$ for the real part and the imaginary part, respectively. The rationing of $\mathbf{f}_{\boldsymbol{\theta}}$ into $\widehat{f}_{\boldsymbol{\theta},n}$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta},n}$ is because the DNN cannot find the complex-valued function $\mathbf{f}_{\boldsymbol{\theta}}$ directly. Instead, the DNN will find two real-valued functions $\widehat{\mathbf{f}}_{\boldsymbol{\theta},n}$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta},n}$, where $\widehat{\mathbf{f}}_{\boldsymbol{\theta},n} = \Re\{\mathbf{f}_{\boldsymbol{\theta}}\}$ and $\widetilde{\mathbf{f}}_{\boldsymbol{\theta},n} = \Im\{\mathbf{f}_{\boldsymbol{\theta}}\}$.

On the basis of what is discussed above, we can now convert the problem (10) into the following form:

$$\underset{\boldsymbol{\psi}_{\boldsymbol{\theta}}=\{\psi_{\boldsymbol{\theta},k}\}_{k=1}^{K_{\mathtt{R}}},\mathbf{f}_{\boldsymbol{\theta}}}{\text{minimize}} \quad -\frac{1}{B}\sum_{t=1}^{B} C_s\left(\boldsymbol{\psi}_{\boldsymbol{\theta}}, \mathbf{f}_{\boldsymbol{\theta}} \,\middle|\, \mathcal{S}_{\text{est}}^{[t]}\right) \triangleq L\left(\boldsymbol{\theta}\right) \tag{13a}$$

$$\text{subject to} \quad \|\mathbf{f}_{\boldsymbol{\theta}}\|^2 = 1 \text{ and } 0 \leq \psi_{\boldsymbol{\theta},k} \leq 1, \tag{13b}$$

where $L\left(\boldsymbol{\theta}\right)$ is defined as the loss function. Note that the DNN actually learns to solve the functional optimization problem (13) rather than the original problem (10). The main difference between the two problems is as follows: $\boldsymbol{\psi}_{\boldsymbol{\theta}}$ and $\mathbf{f}_{\boldsymbol{\theta}}$ in (13) are $\boldsymbol{\theta}$-parameterized functions, while $\boldsymbol{\psi}$ and $\mathbf{f}$ in (13) are not parameterized. Since each element of $\boldsymbol{\psi}_{\boldsymbol{\theta}}$, as well as each element of $\mathbf{f}_{\boldsymbol{\theta}}$, is a parameterized function, the DNN is thus trained to find the suitable values of $\boldsymbol{\theta}$ that satisfy (13).

1) The iterative algorithm applied to the DNN: Since the training process of the DNN is carried out over multiple epochs and the termination of the process relies upon convergence subject to some tolerance, any solution provided by the DNN can only be deemed to constitute an approximate solution rather than the actual optimal solution to (13). During the training, $\boldsymbol{\theta}$ will be updated iteratively. Upon denoting the value of $\boldsymbol{\theta}$ at the ϵ-th epoch by $\boldsymbol{\theta}_{[\epsilon]}$ and the learning rate of the DNN by λ, and then using the *stochastic gradient descent* (SGD) algorithm, we can calculate the value of $\boldsymbol{\theta}$ at the $(\epsilon{+}1)$-st epoch as

$$\boldsymbol{\theta}_{[\epsilon+1]} = \boldsymbol{\theta}_{[\epsilon]} + \frac{\lambda}{B}\sum_{t=1}^{B} \nabla_{\boldsymbol{\theta}} C_s\left(\boldsymbol{\psi}_{\boldsymbol{\theta}}, \mathbf{f}_{\boldsymbol{\theta}} \,\middle|\, \mathcal{S}_{\text{est}}^{[t]}\right)\Bigg|_{\substack{\boldsymbol{\psi}_{\boldsymbol{\theta}}=\boldsymbol{\psi}^{[t,\epsilon]} \\ \mathbf{f}_{\boldsymbol{\theta}}=\mathbf{f}^{[t,\epsilon]}}}. \tag{14}$$

The convergence analysis of DNNs relying on the SGD can be found in [20, Proposition 1] and references therein. Since the SGD update in (14) implies a loop over multiple iterations, we set up the stopping criterion based on a sufficiently large number of iterations given a predetermined threshold.

2) The architecture of the DNN: In order to facilitate the implementation with the aid of the open-source framework `tensorflow`, it is necessary to construct the input data for ensuring that the arrangement of each sample complies with the requirements of the framework. Accordingly, the t-th sample $\mathcal{S}_{\text{est}}^{[t]}$ will be arranged in the row format as follows:

$$\mathbf{x}_{\text{raw}}^{[t]} = \left[\mathbf{r}_1[t], \ldots, \mathbf{r}_{K_{\mathtt{R}}}[t], \mathbf{h}_{\mathtt{RB}}[t], \mathbf{h}_{\mathtt{AB}}[t], \mathbf{h}_{\mathtt{RE}}^{\text{est}}[t], \mathbf{h}_{\mathtt{AE}}^{\text{est}}[t]\right], \tag{15}$$

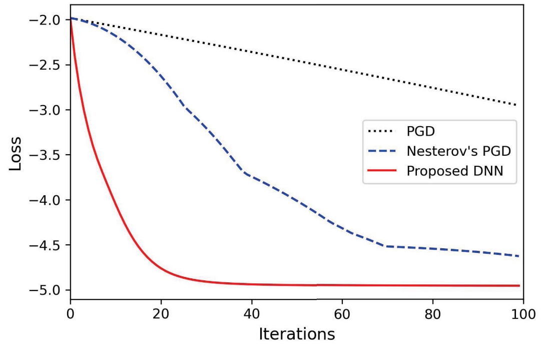

Fig. 2: The convergence of the proposed DNN compared to the projected gradient descent (PGD) and the Nesterov's PGD.

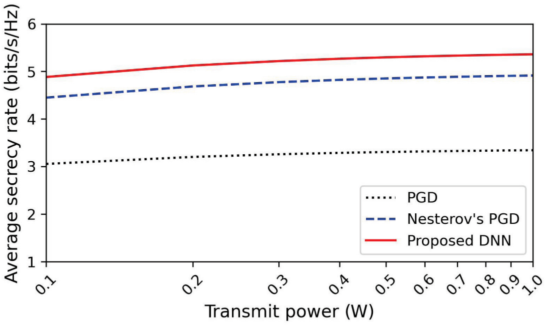

Fig. 3: The average secrecy rate versus the transmit power in 3 different schemes.

where $\mathbf{r}_k[t] \in \mathbb{C}^{1\times N_{\mathtt{A}}}$ denotes the k-th row vector of $\mathbf{H}_{\mathtt{AR}}[t]$, with $k \in \{1,\ldots,K_{\mathtt{R}}\}$. Note that $\mathbf{x}_{\text{raw}}^{[t]} \in \mathbb{C}^{1\times(N_{\mathtt{A}}K_{\mathtt{R}}+2K_{\mathtt{R}}+2N_{\mathtt{A}})}$ is a complex-valued row vector. Since the state-of-the-art DNN architectures are typically designed for real numbers, we will arrange the input data of the DNN as

$$\mathbf{x}_{\text{in}}^{[t]} = \left[\Re\left\{\mathbf{x}_{\text{raw}}^{[t]}\right\}, \Im\left\{\mathbf{x}_{\text{raw}}^{[t]}\right\}\right] \in \mathbb{R}^{1\times(2N_{\mathtt{A}}K_{\mathtt{R}}+4K_{\mathtt{R}}+4N_{\mathtt{A}})}. \quad (16)$$

As for the output of the DNN, we also use a real-valued row vector to host the content of the output. In particular, the output will be designed as follows:

$$\mathbf{y}_{\text{out}}^{[t,\epsilon]} = \Bigg[\underbrace{y_1^{[t,\epsilon]},\ldots,y_{K_{\mathtt{R}}}^{[t,\epsilon]}}_{\text{relating to } \boldsymbol{\psi}^{[t,\epsilon]}}, \underbrace{y_{K_{\mathtt{R}}+1}^{[t,\epsilon]},\ldots,y_{K_{\mathtt{R}}+2N_{\mathtt{A}}}^{[t,\epsilon]}}_{\text{relating to } \widehat{\mathbf{f}}^{[t,\epsilon]} \text{ and } \widetilde{\mathbf{f}}^{[t,\epsilon]}}\Bigg]. \quad (17)$$

The first $K_{\mathtt{R}}$ nodes of the output layer are activated by the `sigmoid` functions so that $0 \le y_k^{[t,\epsilon]} \le 1$, $k \in \{1,\ldots,K_{\mathtt{R}}\}$. As a result, we can assign $\boldsymbol{\psi}^{[t,\epsilon]} = \left[y_1^{[t,\epsilon]},\ldots,y_{K_{\mathtt{R}}}^{[t,\epsilon]}\right]$, while the remaining $2N_{\mathtt{A}}$ nodes of the output layer are activated by the `linear` functions so that $-\infty \le y_k^{[t,\epsilon]} \le \infty$, $k \in \{K_{\mathtt{R}}+1,\ldots,K_{\mathtt{R}}+2N_{\mathtt{A}}\}$. Upon defining $\widehat{\mathbf{f}}_{\text{raw}}^{[t,\epsilon]} \triangleq \left[y_{K_{\mathtt{R}}+1}^{[t,\epsilon]},\ldots,y_{K_{\mathtt{R}}+N_{\mathtt{A}}}^{[t,\epsilon]}\right]$, $\widetilde{\mathbf{f}}_{\text{raw}}^{[t,\epsilon]} \triangleq \left[y_{K_{\mathtt{R}}+N_{\mathtt{A}}}^{[t,\epsilon]},\ldots,y_{K_{\mathtt{R}}+2N_{\mathtt{A}}}^{[t,\epsilon]}\right]$ and $\mathbf{f}_{\text{raw}}^{[t,\epsilon]} \triangleq \widehat{\mathbf{f}}_{\text{raw}}^{[t,\epsilon]} + \sqrt{-1}\,\widetilde{\mathbf{f}}_{\text{raw}}^{[t,\epsilon]}$, we can find $\mathbf{f}^{[t,\epsilon]}$ from $\mathbf{f}_{\text{raw}}^{[t,\epsilon]}$ by the classic projection method [21]

$$\mathbf{f}^{[t,\epsilon]} = \underset{\mathbf{z}\in\mathcal{C}}{\arg\min}\, \|\mathbf{z} - \mathbf{f}_{\text{raw}}^{[t,\epsilon]}\|, \quad (18)$$

where $\mathcal{C} = \{\mathbf{z} \in \mathbb{C}^{1\times N_{\mathtt{A}}} : \|\mathbf{z}\|^2 \le 1\}$ is a constraint set that is explicitly deduced from the constraint (13a).

IV. Numerical Results

In this section, we will offer numerical examples for quantifying the security performance of the RIS-aided AANET with the help of the projection-based DNN. **Simulation parameters:** We model the path loss as

$$\mathfrak{L}_{\mathtt{A}j}\ [\text{dB}] = -154.06 + 20\log_{10}(f_c) + 20\log_{10}(d_{\mathtt{A}j}), \quad (19)$$

where f_c [Hz] is the operating SHF, and $d_{\mathtt{A}j}$ [m] is the distance from $\mathtt{A}$ to $j \in \{\mathtt{B},\mathtt{E},\mathtt{RB},\mathtt{RE}\}$. In our simulations, we set $f_c = 3$ GHz, $d_{\mathtt{AB}} = 9$ km, $d_{\mathtt{AE}} = 10$ km, $d_{\mathtt{ARB}} = 9.05$ km, and $d_{\mathtt{ARE}} = 10.05$ km. We model the noise variance N_0 as $N0 = \text{BW} \times \varpi_{\text{Boltzmann}} \times \varpi_{\text{temp}} \times \varpi_{\text{fig}}$, where BW is the bandwidth in Hz, $\varpi_{\text{Boltzmann}} = 1.38 \times 10^{-23}$ (Joule/Kelvin) is the Boltzmann constant, ϖ_{temp} is the noise temperature in Kelvin, and ϖ_{fig} is the noise figure in dB. In our simulations, we set $\text{BW} = 5$ MHz, $\varpi_{\text{temp}} = 290$ Kelvin and $\varpi_{\text{fig}} = 9$ dB. Concerning the Doppler effect, we set $v_{\mathtt{B}} = 200$ m/s, $v_{\mathtt{E}} = 180$ m/s and $f_{\text{Baud}} = 625$ kHz. Unless otherwise specified, the default values of the other system parameters are as follows: $N_{\mathtt{A}} = 5$ antennas, $K_{\mathtt{R}} = 5$ elements, $\kappa = 5$, $\zeta = 0.2$, the learning rate is $\lambda = 0.001$, the number of hidden layers is 4, each hidden layer has 60 neurons, the batch size is $|\mathcal{B}| = B = 500$ samples. The dataset that is used as the DNN input data is the set $\{\mathbf{x}_{\text{in}}^{[t]}\}_{t=1}^{B}$, where the t-th input sample $\mathbf{x}_{\text{in}}^{[t]}$ is defined in (16). Recall that $\mathbf{x}_{\text{in}}^{[t]}$ contains the real and imaginary parts of the channel observations at the t-th time slot (see the formation of $\mathbf{x}_{\text{in}}^{[t]}$ from $\mathcal{S}_{\text{est}}^{[t]}$ through the expressions (8), (15) and (16)).

Fig. 2 compares the convergence of the proposed deep unsupervised learning algorithm to a pair of two conventional algorithms, i.e., the projected gradient descent (PGD) and the Nesterov's PGD [10]. It is clear that our algorithm converges faster than the conventional ones, requiring less iterations to converge to some local optima. Fig. 3 shows the average secrecy rate $\overline{C_s}(\boldsymbol{\psi},\mathbf{f})$ versus the transmit power $P_{\mathtt{A}}$ for three different schemes. It is shown that the security performance is also improved upon increasing $P_{\mathtt{A}}$, but gradually saturates at high $P_{\mathtt{A}}$. Moreover, the proposed system exhibits the highest security performance for the projection-based DNN, while the PGD results in the worst performance.

In general, the superiority of the DNN over its conventional counterparts is because the DNN is capable of learning the complex functional relationship between the channel-based data and the target variables $\{\boldsymbol{\psi},\mathbf{f}\}$ by approximately adjusting the DNN parameters. In other words, the DNN can output $\{\boldsymbol{\psi},\mathbf{f}\}$ as the parameterized functions of the data and find the updated solutions quite promptly, when the dataset is changed. Thus, in the next two figures, we will only consider the proposed DNN. To be more specific, in Fig. 4, we also depict $\overline{C_s}(\boldsymbol{\psi},\mathbf{f})$ w.r.t $P_{\mathtt{A}}$, where two cases are considered: i) without RIS and ii) with RIS $K_{\mathtt{R}} = \{5, 10, 15\}$. In both cases, $\overline{C_s}(\boldsymbol{\psi},\mathbf{f})$ increases with $P_{\mathtt{A}}$. Moreover, $\overline{C_s}(\boldsymbol{\psi},\mathbf{f})$ also increases with $K_{\mathtt{R}}$. Hence, the security performance is the

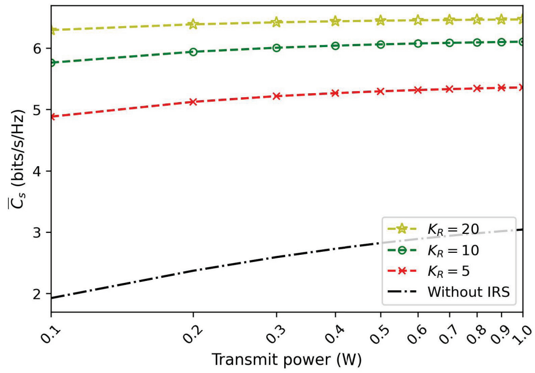

Fig. 4: The average secrecy rate versus the transmit power.

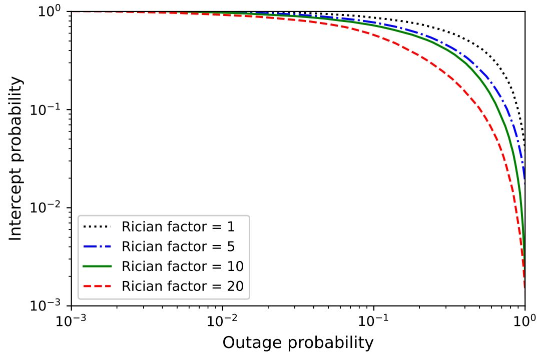

Fig. 5: The intercept probability versus the outage probability.

worst in the case of no RIS, i.e. the integration of the RIS into the AANET improves the security level of the system.

Fig. 5 shows the intercept probability (IP) versus the outage probability (OP) at $N_{\mathrm{A}} = 5$ and $K_{\mathrm{R}} = 5$. Herein, the IP is defined as $\Pr\{\log_2(1+\mathit{\Gamma}_{\mathrm{E}}) \geq p\}$ with p ranging from 0 to 1, while the OP is defined as $\Pr\{\log_2(1+\mathit{\Gamma}_{\mathrm{B}}) \leq p\}$. Additionally, the effect of the Rician factor κ is also taken into account, given its importance in modelling the channel fading of the AANET. Observe from Fig. 5 that at a fixed κ, there is an IP-versus-OP trade-off, because the IP increases when the OP decreases and vice versa. This means that we accept a higher probability of incorrectly detecting signals at $\mathtt{B}$ in return for a system with a higher probability of security. However, both the IP and the OP are reduced when κ increases, indicating that the more influence the LoS component has, the higher the security level of the RIS-aided AANET.

V. Conclusions

In this paper, we considered a RIS-aided AANET and designed a deep unsupervised learning algorithm for maximizing the average secrecy rate. The proposed algorithm relied on a projection-based DNN, which outperformed a pair of conventional schemes, namely, the PGD and the PGD using Nesterov's acceleration. The results showed that the employment of the RIS improved the security of the system. Finally, the security was also further enhanced in the case of having stronger LoS.

References

[1] X. Huang, J. A. Zhang, R. P. Liu, Y. J. Guo, and L. Hanzo, "Airplane-aided integrated networking for 6G wireless: Will it work?" *IEEE Veh. Tech. Mag.*, vol. 14, no. 3, pp. 84–91, 2019.

[2] Y. A. Nijsure, G. Kaddoum, G. Gagnon, F. Gagnon, C. Yuen, and R. Mahapatra, "Adaptive air-to-ground secure communication system based on ADS-B and wide-area multilateration," *IEEE Trans. on Veh. Tech.*, vol. 65, no. 5, pp. 3150–3165, 2016.

[3] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[4] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wirel. Commun. Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[5] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning based intelligent reflecting surface for secure wireless communications," *IEEE Trans. on Wireless Communications*, pp. 1–1, 2020.

[6] Y. Song, M. R. Khandaker, F. Tariq, and K.-K. Wong, "Truly intelligent reflecting surface-aided secure communication using deep learning," *arXiv preprint arXiv:2004.03056*, 2020.

[7] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Sig. Process. Lett.*, vol. 27, pp. 1300–1304, 2020.

[8] L. Dong, H.-M. Wang, and H. Xiao, "Secure cognitive radio communication via intelligent reflecting surface," *IEEE Trans.on Commun.*, vol. 69, no. 7, pp. 4678–4690, 2021.

[9] S. Zhang, Y. Xia, and J. Wang, "A complex-valued projection neural network for constrained optimization of real functions in complex variables," *IEEE Trans.on Neu Net. and Learning Sys.*, vol. 26, no. 12, pp. 3227–3238, 2015.

[10] S. Bubeck, "Convex optimization: Algorithms and complexity," *Found. Trends Mach. Learn.*, vol. 8, no. 3–4, p. 231–357, Nov. 2015.

[11] N. J. Earnhardt Jr, S. F. Bauler, W. T. Greenleaf, and J. M. Wichgers, "Remotely-managed aircraft RF communication network, device, and method," 2019, US Patent 10,425,150.

[12] C. Shao, W. Jang, H. Park, J. Sung, Y. Jung, and W. Lee, "Phantom eavesdropping with whitened RF leakage," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 2, pp. 232–235, 2020.

[13] Y. Chen, L. Wang, Y. Ai, B. Jiao, and L. Hanzo, "Performance analysis of NOMA-SM in vehicle-to-vehicle massive MIMO channels," *IEEE J. on Sel. Areas in Commun.*, vol. 35, no. 12, pp. 2653–2666, 2017.

[14] S. Noh, M. D. Zoltowski, Y. Sung, and D. J. Love, "Pilot beam pattern design for channel estimation in massive MIMO systems," *IEEE J. of Selected Topics in Sig. Process.*, vol. 8, no. 5, pp. 787–801, 2014.

[15] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. USA: Academic Press, 2007.

[16] J. Li, D. Wang, P. Zhu, and X. You, "Uplink spectral efficiency analysis of distributed massive MIMO with channel impairments," *IEEE Access*, vol. 5, pp. 5020–5030, 2017.

[17] H.-N. Lee, "Adaptive diversity combining, equalization and sequence decoding for time-varying dispersive channels," Ph.D. dissertation, UCLA, 1999.

[18] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Secure massive mimo under imperfect csi: Performance analysis and channel prediction," *IEEE Trans. on Information Forensics and Security*, vol. 14, no. 6, pp. 1610–1623, 2019.

[19] L. Dong and H.-M. Wang, "Enhancing secure MIMO transmission via intelligent reflecting surface," *IEEE Trans.on Wirel. Commun.*, vol. 19, no. 11, pp. 7543–7556, 2020.

[20] H. Lee, S. H. Lee, and T. Q. S. Quek, "Deep learning for distributed optimization: Applications to wireless resource management," *IEEE J. on Sel. Areas in Commun.*, vol. 37, no. 10, pp. 2251–2266, 2019.

[21] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.