A Novel Design of RIS for Enhancing the Physical Layer Security for RIS-aided NOMA Networks

Zhiqing Tang, *Student Member, IEEE,* Tianwei Hou, *Member, IEEE,* Yuanwei Liu, *Senior Member, IEEE,* Jiankang Zhang, *Senior Member, IEEE,* and Caijun Zhong, *Senior Member, IEEE*

***Abstract*—This letter proposes a novel design of reconfigurable intelligent surface (RIS) to enhance the physical layer security (PLS) in the RIS-aided non-orthogonal multiple access (NOMA) network. Under the design of the RIS, the problem of increasing the number of RIS elements damaging the secrecy performance is solved. Besides, it also ensures that the networks can use traditional channel coding schemes to achieve secrecy. Our results show that the novel design of the RIS is ready for enhancing secrecy performance.**

***Index Terms*—Non-orthogonal multiple access, physical layer security, reconfigurable intelligent surface.**

I. Introduction

DUE to the superior spectrum efficiency (SE), non-orthogonal multiple access (NOMA) will play an important role in 5G and beyond. Compared with the conventional orthogonal multiple access (OMA) network structure, NOMA has the outstanding ability to strengthen the SE and user connectivity [1]. Since the signals are broadcast in wireless communication networks, it is equally important to guarantee the confidentiality of communication going on between the base station (BS) and legitimate users (LUs).

In recent times, a new technology which has the ability to manage the reflection properties of the radio waves, named reconfigurable intelligent surface (RIS), has been proposed [2]. By properly adapting the amplitude-reflection and phase coefficients, the RIS can enhance or reduce the received signals by users [3], [4], which provides more possibilities for physical layer security issues. In [5], the authors studied the secrecy outage probability (SOP) of an RIS-aided wireless network, and revealed that the RIS make a motion to boost the secrecy performance. The PLS of a vehicular network with the assisted of the RIS has been studied in [6]. In [7], the authors analyzed the SOP of the RIS-aided NOMA network with multi-user. However, considering the PLS for the RIS-aided NOMA network, in which both the direct link and reflected links exist, still have few reported in the literature.

We first put forward a new RIS-aided NOMA network, in which a BS communicates with M LUs and an eavesdropper (Eve) via the assisted of the RIS. It is worth noting that most of the literature, such as [6], [7], the designs of RIS for enhancing the performance of LU. However, we propose a new design of the RIS for eliminating the signals received by the Eve to enhance the secrecy performance, which gives a new direction for the PLS design of communication networks.

II. System Model

We consider a secure downlink (DL) RIS-aided NOMA network which includes a BS, an RIS, M LUs and an Eve. In the network considered, there are direct links between the BS and LUs as well as Eve, and the BS also communicates with LUs and Eve by means of the RIS. We assume that the RIS has K (K is large enough[1]) elements, positioned at the appropriate location. Similar to [8], we assume that the Eve has a powerful detection capability. We also assume that the BS and all the users, include LUs and Eve, are equipped with a single antenna. Moreover, we consider that only two randomly chosen users can share an orthogonal resource block to communicate with the BS in NOMA.

For simplicity, we assume that the selected NOMA users and the Eve are denoted by m, n ($m, n \in (1, 2, \cdots, M)$) and e, respectively. The distances between user i ($i \in \{m, n, e\}$) and the BS as well as the RIS are denoted by $d_{d,i}$ and $d_{r,i}$, respectively. Practically, the positions of the BS and the RIS are settled. Therefore, we consider that the distance between the BS and the RIS is fixed, denoted by d_1. Therefore, the large-scale fading of the reflected links for user i can be expressed by $L_i = d_1^{-\alpha_1} d_{r,i}^{-\alpha_{r,i}}$, where α_1 and $\alpha_{r,i}$ are the path loss exponents.

The small-scale fading is denoted by $\mathbf{h}_r$ to describe the channel between the BS and the RIS, where $\mathbf{h}_r = [h_{r,1}, h_{r,2}, \ldots, h_{r,K}]^T$ is a $K \times 1$ vector, whose elements follow the Nakagami-m distribution with fading parameter t_1. Moreover, the small-scale fading between user i and the RIS can be expressed by $\mathbf{g}_i = [g_{i,1}, g_{i,2}, \ldots, g_{i,K}]$, whose elements follow the Nakagami-m distribution with fading parameter $t_{r,i}$. Because of the complicated scattering environment, the direct

This work was supported by the National Natural Science Foundation of China under Grant 61571401 and 61901416. *(Corresponding authors: Yuanwei Liu; Jiankang Zhang.)*

Z. Tang is with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China (email:iezqtang@zzu.edu.cn).

T. Hou is with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China (email:twhou@bjtu.edu.cn).

Y. Liu is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, UK (email:yuanwei.liu@qmul.ac.uk).

J. Zhang is with the Department of Computing & Informatics, Bournemouth University, Poole BH12 5BB, U.K. (E-mail: jzhang3@bournemouth.ac.uk).

C. Zhong is with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310007, China (email:caijunzhong@zju.edu.cn).

[1]In order to eliminate the signal received at Eve, similar to Lemma 1 in [4], the number of RIS elements needs to meet the condition of $K^2 \geq d_{d,e}^{-\alpha_{d,e}} / L_e$, which is beyond our research content of this letter.

links between user i and the BS follow the Rayleigh fading, are denoted by h_i, and we assume that h_m, h_n and h_e are independent and unrelated.

The BS sends $\mathbf{s} = \sqrt{a_m}s_m + \sqrt{a_n}s_n$ to the paired NOMA users, where s_m and s_n denote the signal aim to user m and user n, respectively. While $\sqrt{a_m}$ and $\sqrt{a_n}$ representing the power allocation factors, respectively. Therefor, the signal received from the BS for user i can be expressed by

$$y_i = \left(\mathbf{g}_i \Phi \mathbf{h}_r \sqrt{L_i} + h_i \sqrt{d_{d,i}^{-\alpha_{d,i}}}\right) P\mathbf{s} + N_i, \tag{1}$$

where P is the transmit power of the BS, $\Phi \triangleq \text{diag}[\beta_1\phi_1, \beta_2\phi_2, \ldots, \beta_K\phi_K]$ is the response matrix of the RIS, which includes the phase shift ϕ_k and the amplitude reflection coefficient β_k, and $\alpha_{d,i}$ denotes the path loss exponent of the BS to user i. Finally, $N_i \sim (0, \sigma_i^2)$ denotes the additive white Gaussian noise (AWGN) at user i.

III. Eliminating the Threat of Eve with RIS

In this section, we force our attention on the design of RIS to eliminate the risk of information be eavesdropped, then we analyze its secrecy performance. Specifically, in order to simultaneously control the RIS, we consider the global CSI, as in [9], can be perfectly available.

A. RIS Design

In this subsection, we force our attention to design the response matrix of the RIS. The channel gain of the i-th user can be expressed by

$$|\tilde{h}_i|^2 = \left|\mathbf{g}_i \Phi \mathbf{h}_r \sqrt{L_i} + h_i \sqrt{d_{d,i}^{-\alpha_{d,i}}}\right|^2. \tag{2}$$

To enhance the network's secrecy rate, we can reach it from the next two aspects: 1) by enhancing the capacity of LUs; 2) by reducing the capacity of Eve. In this letter, we consider the second way to enhance the PLS of RIS-aided NOMA network. The design of the RIS as follows:

$$\mathbf{g}_m \Phi \mathbf{h}_r \sqrt{L_m} = 0, \tag{3a}$$

$$\mathbf{g}_n \Phi \mathbf{h}_r \sqrt{L_n} = 0, \tag{3b}$$

$$\mathbf{g}_e \Phi \mathbf{h}_r \sqrt{L_e} = -h_e \sqrt{d_{d,e}^{-\alpha_{d,e}}}. \tag{3c}$$

It is worth mentioning that since the design of (3c) is for eliminating the signals received by the Eve. Therefore, it is difficult to evaluate the channel gains of LUs. In order to prevent the direct signals and reflected signals received at LUs mutual elimination, we propose a feasible proposal as (3a) and (3b).

Therefore, we can rewrite (3) as

$$\tilde{\mathbf{H}}_{\text{D}} \tilde{\Phi} = \mathbf{b}, \tag{4}$$

where $\mathbf{b} = \left[0, 0, -h_E \sqrt{d_E^{-\alpha_E}}\right]^{\text{T}}$, $\tilde{\Phi} = \Phi[1, \cdots, 1]^{\text{T}}$ and

$$\tilde{\mathbf{H}}_{\text{D}} = \begin{bmatrix} g_{m,1}h_{r,1}\sqrt{L_m} & \cdots & g_{m,K}h_{r,K}\sqrt{L_m} \\ g_{n,1}h_{r,1}\sqrt{L_n} & \cdots & g_{n,K}h_{r,K}\sqrt{L_n} \\ g_{e,1}h_{r,1}\sqrt{L_e} & \cdots & g_{e,K}h_{r,K}\sqrt{L_e} \end{bmatrix}. \tag{5}$$

To reach the targets design purpose, the global solution of (4) can be expressed as

$$\tilde{\Phi} = \text{pinv}(\tilde{\mathbf{H}}_{\text{D}})\mathbf{b}, \tag{6}$$

where $\text{pinv}(\tilde{\mathbf{H}}_{\text{D}})$ represents the pseudo-inverse of the matrix $\tilde{\mathbf{H}}_{\text{D}}$. Thus, we can obtain $\Phi = \text{diag}(\tilde{\Phi})$.

B. New Channel Statistics

Let us denote $\hat{\lambda}_m$ and $\hat{\lambda}_n$ are the channel gains of user m and n, respectively. Generality, we assume that $\hat{\lambda}_1 \leq \cdots \leq \hat{\lambda}_m \leq \cdots \leq \hat{\lambda}_n \cdots \leq \hat{\lambda}_M$. Substituting (3a) and (3b) into (1), the instantaneous signal-to-noise ratio (SNR) of user m and n can be written as

$$\gamma_m = \frac{a_m \hat{\lambda}_m}{a_n \hat{\lambda}_m + \frac{1}{\rho_b}}, \tag{7}$$

$$\gamma_n = \rho_b a_n \hat{\lambda}_n, \tag{8}$$

respectively, where $\rho_b = \frac{P}{\sigma_i^2}$ is the transmit SNR.

Lemma 1. *Based on the design of the RIS, the cumulative distribution function (CDF) of γ_n can be written as*

$$F_{\gamma_n}(x) = \varphi_n \sum_{q=0}^{M-n} \binom{M-n}{q} \frac{(-1)^q}{n+q} \left(1 - e^{-\frac{\epsilon_n x}{a_n \rho_b}}\right)^{n+q}, \tag{9}$$

where $\varphi_n = \frac{M!}{(M-n)!(n-1)!}$ and $\epsilon_n = d_{d,n}^{\alpha_{d,n}}$.

Proof. Denote λ_n as the disordered channel gain of the BS to user n, and it is exponentially distributed random variables (RVs) with parameter $\epsilon_n = d_{d,n}^{\alpha_{d,n}}$. The CDF of $F_{\lambda_n}(x)$ is

$$F_{\lambda_n}(x) = 1 - e^{-\frac{\epsilon_n x}{a_n \rho_b}}. \tag{10}$$

Let $\hat{\lambda}_n$ as the ordered channel gain of the BS to the n-th user links. Based on [8], we have

$$F_{\hat{\lambda}_n}(x) = \varphi_n \sum_{q=0}^{M-n} \binom{M-n}{q} \frac{(-1)^q}{n+q} \left(F_{\lambda_n}(x)\right)^{n+q}. \tag{11}$$

By substituting (10) into (11), (9) can be obtained. □

Lemma 2. *Based on the design of the RIS, the CDF of γ_m is*

$$F_{\gamma_m}(x) = H(x - \frac{a_m}{a_n}) + H(\frac{a_m}{a_n} - x)\varphi_m \times \sum_{q=0}^{M-m} \binom{M-m}{q} \frac{(-1)^q}{m+q} \left(1 - e^{-\frac{\epsilon_m x}{(a_m - a_n x)\rho_b}}\right)^{m+q}, \tag{12}$$

where $\varphi_m = \frac{M!}{(M-m)!(m-1)!}$, $\epsilon_m = d_{d,m}^{\alpha_{d,m}}$ *and* $H(x) = \begin{cases} 1, x > 0 \\ 0, x \leq 0 \end{cases}$ *is the unit step function.*

Proof. The CDF of $F_{\gamma_m}(x)$ can be expressed as

$$F_{\gamma_m}(x) = \begin{cases} \underbrace{Pr\left\{\hat{\lambda}_m < \frac{x}{\rho_b(a_m - a_n x)}\right\}}_{\Phi_B}, & x < \frac{a_m}{a_n} \\ 1, & x \geq \frac{a_m}{a_n}. \end{cases} \tag{13}$$

Let us denote λ_m as the disordered channel gain of the BS to the m-th user links, and it is exponentially distributed RVs with parameter $\epsilon_m = d_{d,m}^{\alpha_{d,m}}$. In the case of $x < \frac{a_m}{a_n}$, the CDF of $F_{\gamma_m}(x)$ is

$$F_{\lambda_m}(x) = 1 - e^{-\frac{\epsilon_m x}{(a_m - a_n x)\rho_b}}. \tag{14}$$

Based on [8], Φ_B can be expressed as

$$\Phi_B = \varphi_m \sum_{q=0}^{M-m} \binom{M-m}{q} \frac{(-1)^q}{m+q} \left(F_{\lambda_m}(x)\right)^{m+q}. \tag{15}$$

By substituting (15) and (14) into (13), then through the medium of the unit step function, (12) can be obtained. □

Remark 1. *Based on the design of the RIS, the capacity of the Eve is zero.*

C. Performance Analysis

According to the network described above, the capacity of user ℓ can be expressed as $C_{U_\ell} = \log_2(1+\gamma_\ell)$. While the capacity of the Eve, based on the design of the RIS, is given by $C_{e,\ell} = \log_2(1+\gamma_{e,\ell})$. The secrecy rate of user ℓ is defined by $C_\ell = [C_{U_\ell} - C_{E_\ell}]^+$, where $[x]^+ = \max[x, 0]$. The SOP is defined by the probability that the secrecy rate less than R_ℓ, who is a given secrecy rate.

Under the proposed design of the RIS, the capacity of eavesdropping channel is forced to zero, there is no secrecy issue at all. However, based on the definitions of secrecy rate and SOP, we can consider that the outage probability is a special case of SOP when the capacity of the eavesdropper and R_ℓ are zero.

To compare with the secrecy outage probability, we define a special outage probability.

Definition 1. *Special outage probability is the probability when the capacity of user ℓ less than R_ℓ.*

Theorem 1. *Given the ordered channel gains, the special outage probability of user n is*

$$P_n(R_n) = \varphi_n \sum_{q=0}^{M-n} \binom{M-n}{q} \frac{(-1)^q}{n+q} \left(1 - e^{-y_n}\right)^{n+q}, \tag{16}$$

where $y_n = \frac{\epsilon_n\left(2^{R_n}-1\right)}{a_n \rho_b}$.

Proof. Based on the definition of special outage probability and **Lemma 1**, it is easy to obtain (16). □

Theorem 2. *Given the ordered channel gains, in the case of $\frac{a_m}{a_n} > 2^{R_m} - 1$, the special outage probability of user m is*

$$P_m(R_m) = \varphi_m \sum_{q=0}^{M-m} \binom{M-m}{q} \frac{(-1)^q}{m+q} \left(1 - e^{-y_m}\right)^{m+q}, \tag{17}$$

where $y_m = \frac{\epsilon_m\left(2^{R_m}-1\right)}{\left(a_m - a_n\left(2^{R_m}-1\right)\right)\rho_b}$.

Proof. The proof is akin to **Theorem 1**. □

To derive the diversity order, we have $d_s = -\lim_{\rho_b \to \infty} \log P^\infty / \log \rho_b$, where P^∞ denotes the asymptotic special outage probability.

Corollary 1. *The asymptotic special outage probability of the user n is*

$$P_n^\infty(R_n) = \frac{\varphi_n}{n} y_n^n. \tag{18}$$

Proof. In the case of $y \to 0$, we have $1 - e^{-y} \approx y$. By applying this result to (16), (18) can be obtained. □

Remark 2. *By substituting* (18) *into d_s, the diversity order of user n can be obtained as n.*

Corollary 2. *The asymptotic special outage probability of user m is*

$$P_m^\infty(R_m) = \frac{\varphi_m}{m} y_m^m. \tag{19}$$

Proof. The proof is akin to **Corollary 1**. □

Remark 3. *By substituting* (19) *into d_s, the diversity order of user m can be obtained as m.*

It is worth noting that, based on the design of the RIS, there are no influences on our results by the reflected links and the number of RIS elements. Compared with the transmission strategy proposed in [10], the design of the RIS ensures that the BS can always transmit signals without secrecy outage. The proposed design of the RIS provides insightful guidelines for a novel solution when the channel gains of the Eve are better than that of LUs. Moreover, the proposed design of the RIS not only can solve the issue that increasing the number of RIS elements harms the secrecy performance [7], but also can avoid the need for wiretap codes [11], and the system is able to use conventional channel codes to achieve secrecy.

IV. Numerical Results

In this section, we show the performance of the proposed method for enhancing the PLS. We assumed $a_m = 0.6$, $a_n = 0.4$, and $K = 20$. The bandwidth (BW) is set to 1 MHz, and $\sigma_i^2 = -174 + 10\log_{10}(BW)$ dBm. The power attenuation at the reference distance is set to -30 dB for each link. Targeted rates/secrecy rates are set to $R_m = 1$ Mbps and $R_n = 1.5$ Mbps, respectively. The path loss exponents are set to $\alpha_{d,i} = 4$ and $\alpha_1 = \alpha_{r,i} = 2.2$, respectively. The distance between the BS and the RIS is $d_1 = 80$m. The length of the RIS to the user m, user n and the Eve are set to $d_{r,m} = 160$m and $d_{r,n} = 80$m, and $d_{r,e} = 160$m, respectively. The length of the BS to the user m, user n and the Eve are set to $d_{d,m} = 150$m and $d_{d,n} = 100$m, and $d_{d,e} = 200$m, respectively.

As the benchmark, we consider the traditional NOMA and signal-enhance scheme, where the RIS is deployed to enhance the signals received by the user who has a good direct link [12].

Fig. 1 shows the special outage probability versus the transmit power for different distances. We can observe that by reducing the distance between the BS and LUs result in the decreased special outage probability. This is because that the smaller distance of the direct link leads to a lower path loss. Another observation is that even the channel gain of the direct link for the LUs is poorer than that of the Eve's, the considered network also works.

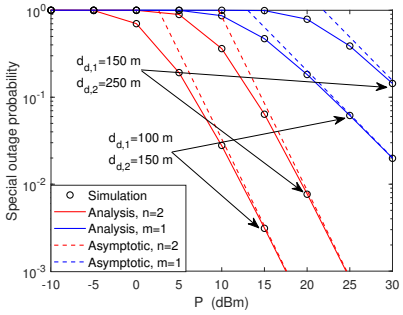

Fig. 1: The special outage probability versus the transmit power for different distances in the case of $M = 2$.

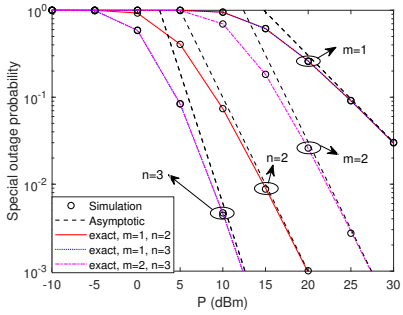

Fig. 2: The special outage probability versus the transmit power for different selected user pair in the case of $M = 3$.

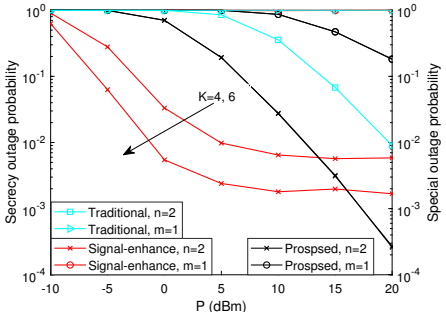

Fig. 3: The comparison between the proposed scheme and the signal-enhance scheme, as well as traditional NOMA.

Fig. 2 plots the special outage probability versus the transmit power for different selected user pair. It can be observed that, for the paired NOMA users, the slope of the special outage probability for user n is higher than that for user m, this is because that the channel gains of user n is better than the channel gains of user m, and the diversity orders of the LUs are decided by the index of the ordered channel gains. This phenomenon is also affirmed by the understandings in **Remark 2** and **Remark 3**.

Fig. 3 shows the SOP of traditional NOMA and signal-enchance scheme, as well as the special outage probability of the proposed scheme versus the transmit power when $K = 4$ and $K = 6$, and we compared the traditional NOMA and the signal-enhance scheme with our proposed scheme. For user n, we observe that the SOP of the signal-enhance scheme is better than the special outage probability of the proposed scheme in low-SNR regions, while the the special outage probability of the proposed scheme is better than the SOP of the signal-enhance scheme in the high-SNR regions. We also observe that with the increase of K, the SOP of the signal-enhance scheme decrease, while the special outage probability of the proposed scheme for both $K = 4$ and $K = 6$ are equal. It is because that the SOP tends to the floor with the transmit SNR increasing. However, with the increase of transmit power, the the special outage probability of proposed scheme decrease. Moreover, the number of the RIS elements K has no effect on the the special outage probability of the proposed scheme. For user m, we observe that the SOP of the signal-enhance scheme is 1 for both $K = 4$ and $K = 6$. It is caused by the following reasons: the RIS is designed to enchane the signals received by user n, therefore it acts the same role to user m and Eve. Moreover, the distance from the RIS to user m and EVe are equal. We also observe that the the special outage probability of the proposed scheme for $K = 4$ and $K = 6$ are equal. Furthermore, the SOP curves of the traditional NOMA network are plotted for comparison. We can observe that RIS-aided NOMA networks have superior secrecy performance than traditional NOMA networks. It is because that the design of RIS can eliminate the risk of eavesdropping on information at the Eve.

V. Conclusion

This letter investigated the secrecy performance of RIS-aided NOMA networks. We first proposed a novel design of the RIS to improve the secrecy performance. Then, we derived the analytical expressions of the special outage probability. Also, the diversity orders were provided. Numerical results were provided to verify the accuracy of the analytical results. The secrecy performance of traditional NOMA and signal-enhance RIS-aided NOMA scenarios have been compared, which concluded that the proposed scheme has superior secrecy performance than traditional NOMA and signal-enhance scheme.

References

[1] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Non-orthogonal multiple access for 5G and beyond," *Proc. IEEE.*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[2] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Aug. 2019.

[3] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, Z. Qin, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *arXiv preprint arXiv:2007.03435*, Jul. 2020.

[4] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "MIMO-NOMA networks relying on reconfigurable intelligent surface: A signal cancellation based design," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 6932–6944, Nov. 2020.

[5] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, pp. 1–1, Jul. 2020.

[6] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," *arXiv preprint arXiv:2004.11288*, 2020.

[7] L. Yang and Y. Yuan, "Secrecy outage probability analysis for RIS-assisted NOMA systems," *Electronics Letters*, Oct. 2020.

[8] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, M. Elkashlan, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[9] S. Gong, S. Ma, C. Xing, Y. Li, and L. Hanzo, "Multi-antenna aided secrecy beamforming optimization for wirelessly powered HetNets," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5261 – 5277, Aug. 2020.

[10] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[11] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[12] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen, and L. Hanzo, "Reconfigurable intelligent surface aided NOMA networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2575–2588, Nov. 2020.