Wireless Personal Communications (2022) 122:2145–2160
https://doi.org/10.1007/s11277-021-08985-0

Physical Layer Security of Non Orthogonal Multiple Access Using Reconfigurable Intelligent Surfaces

Faisal Alanazi[1]

Accepted: 9 August 2021 / Published online: 23 September 2021

Abstract
In this paper, we propose to improve the physical layer security of non orthogonal multiple access (NOMA) using reconfigurable intelligent surfaces (RIS). RIS is decomposed in different sets of reflectors dedicated to NOMA users. As reflections reach the *i*th user with the same phase, the transmitter can reduce its power so that the eavesdropper cannot detect its signal. We derive the secrecy outage probability and the Strictly positive secrecy capacity (SPSC) for NOMA systems using RIS for Rayleigh fading channels.

Keywords Non orthogonal multiple access (NOMA) · Rayleigh fading channels · Physical layer security · Secrecy outage probability (SOP) · Probability of strictly positive secrecy capacity (SPSC) · Reconfigurable intelligent surfaces (RIS)

1 Introduction

Reconfigurable intelligent surfaces (RIS) allow to improve the performance of wireless systems and are a good candidate for 6G communications [1, 2]. RIS can be implemented as a reflector between the transmitter and receiver. All reflections have the same phase at the receiver. Therefore, the receiver output is similar to that of the maximum ratio combiner (MRC) [3]. The phase of *k*th reflector depends on channel phase between transmitter and RIS as well as channel phase between RIS and receiver [4]. The number of RIS reflectors can be varied between $N = 8$ and $N = 512$. RIS offers 10–40 dB gain with respect to conventional wireless systems without RIS [5, 6]. RIS can also be implemented at the transmitter to improve the throughput [1]. When RIS is implemented as a transmitter, the phase of reflector depends on channel phase between RIS and receiver. RIS implemented as a transmitter offers 1 dB with respect to RIS implemented as a reflector [1]. However, RIS implemented as a transmitter cannot be used in Non Orthogonal Multiple Access (NOMA) systems since multiple users should be served. In NOMA systems, RIS should be implemented as a reflector where subsets of reflectors are dedicated to the different users [7].

✉ Faisal Alanazi
faisal.alanazi@psau.edu.sa

[1] Prince Sattam Bin Abdulaziz University, Kharj, Riyadh, Saudi Arabia

Physical layer security of orthogonal multiple access (OMA) has been evaluated in [8, 9]. SOP and SPSC of NOMA systems were computed in [10–13]. Security of energy harvesting systems was studied in [14]. PLS of free space optical (FSO) communications was studied in [15]. SOP and SPSC of Multiple Multiple Output (MIMO) systems were evaluated in [16–20]. In this paper, we propose the use of reconfigurable intelligent Surfaces (RIS) to improve the Physical Layer Security (PLS) of Non Orthogonal Multiple Access (NOMA) systems by evaluating the SOP and SPSC. RIS is decomposed in K sets of reflectors serving K users. Each set of reflectors reflects signals towards a given user. RIS contains N_i reflectors dedicated to user i. When RIS is used, all reflections reach the ith user with the same phase. RIS has not been yet used to improve the physical layer security in NOMA systems where the transmitter sends a combination of symbols dedicated to K users and in the presence of an eavesdropper. The ith user U_i has to detect the symbols of remaining $K - i$ users. It performs Successive Interference Cancelation and detects first the symbol of weakest user. Then, it removes the signal of weakest user and detect that of second weakest user. The process is continued until U_i detects its own symbol. We derive the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity (SPSC) of NOMA systems using reconfigurable intelligent surfaces (RIS). We show that the use of RIS improve the security of physical layer by 10–40 dB with respect to conventional NOMA without RIS.

The contributions of the paper are

- Security enhancement of physical layer of NOMA systems using Reconfigurable Intelligent Surfaces (RIS).
- Derivation of the Secrecy Outage Probability (SOP) and the probability of Strictly Positive Secrecy Capacity (SPSC) of NOMA when RIS is deployed as a reflector.
- Comparison of the SOP and SPSC of NOMA systems when RIS is deployed to conventional NOMA without RIS. We show that the use of RIS improves the security of NOMA systems by 20-30 dB with respect to conventional wireless systems without RIS [10–13].

Next section describes the system model. Section 3 and 4 derive the SOP and SPSC in the presence of two and multiple users. Section 5 describes the theoretical and simulation results. Section 6 compares our results to the current literature. Section 7 concludes the paper.

2 System Model

As shown in Fig. 1, we consider a network containing a Base Station (BS), strong and weak NOMA users U_1 and U_2. Let $\sqrt{\beta}h_k$ be the channel gain between BS and the kth reflector of RIS, $\beta = \frac{1}{d^{ple}}$, d is the distance from BS to RIS and ple is the path loss exponent. For Rayleigh channels, h_k is a zero mean complex Gaussian random variable. Let $h_k = a_k e^{-jb_k}$ where $a_k = |h_k|$ and b_k is the phase of h_k. For Rayleigh channels, a_k is Rayleigh distributed with mean $E(a_k) = \frac{\sqrt{\pi}}{2}$ and $E(a_k^2) = 1$ where $E(.)$ is the expectation operator. Let $\sqrt{\beta_i}g_k$ be the channel gain between kth reflector of RIS and U_i where $\beta_i = \frac{1}{d_i^{ple}}$, d_i is the distance from RIS to U_i. Let $g_k = c_k e^{-je_k}$, $c_k = |g_k|$ and e_k is the phase of g_k. For Rayleigh channels, c_k is Rayleigh distributed with $E(c_k) = \frac{\sqrt{\pi}}{2}$ and $E(c_k^2) = 1$. Let $\sqrt{\beta_E}t$ be the channel coefficient

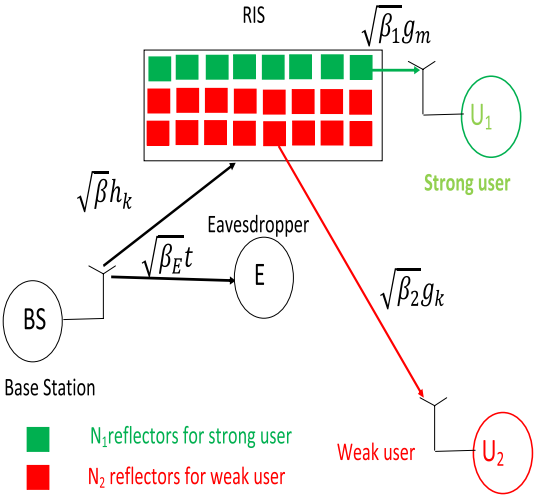

Fig. 1 NOMA using reconfigurable intelligent surfaces (RIS)

between the source and eavesdropper where $\beta_E = \frac{1}{d_E^{ple}}$ and d_E is the distance between source S and E.

RIS adjusts the phase v_k of kth reflector as follows [1]

$$v_k = b_k + e_k. \tag{1}$$

Figure 1 shows that N_1 reflectors are dedicated to user U_1 and N_2 reflectors for user U_2. $N = N_1 + N_2$ is the total number of RIS reflectors. I_1 and I_2 are the set of reflectors dedicated respectively to U_1 and U_2. The received signals at U_1 and U_2 are expressed as

$$r_1 = s\sqrt{2E_s\beta\beta_1}\sum_{k\in I_1} h_k g_k e^{jv_k} + n_1, \tag{2}$$

$$r_2 = s\sqrt{2E_s\beta\beta_2}\sum_{k\in I_2} h_k g_k e^{jv_k} + n_2, \tag{3}$$

where E_s is the symbol energy of BS, s is the transmitted NOMA symbol and n_1, n_2 are Gaussian noises with variance N_0.

The BS transmits a combination of two symbols s_1 and s_2 dedicated to strong and weak users:

$$s = \sqrt{P_1}s_1 + \sqrt{P_2}s_2, \tag{4}$$

where $0 < P_i < 1$ is the power allocated to U_i, $P_1 + P_2 = 1$. More power is allocated to weak user U_2: $0 < P_1 < P_2 < 1$.

Using (1)–(3), we obtain

$$r_1 = s\sqrt{2E_s\beta\beta_1}\sum_{k\in I_1} a_k c_k + n_1, \tag{5}$$

$$r_2 = s\sqrt{2E_s\beta\beta_2}\sum_{k\in I_2} a_k c_k + n_2, \tag{6}$$

Therefore, we have

$$r_1 = \sqrt{A_1}s + n_1, \tag{7}$$

$$r_2 = \sqrt{A_2}s + n_2, \tag{8}$$

where

$$A_1 = 2E_s\beta\beta_1 W_1^2, \tag{9}$$

$$A_2 = 2E_s\beta\beta_2 W_2^2, \tag{10}$$

$$W_1 = \sum_{k\in I_1} a_k c_k, \tag{11}$$

and

$$W_2 = \sum_{k\in I_2} a_k c_k \tag{12}$$

Using (4-6), we have

$$r_1 = \sqrt{A_1}\left[\sqrt{P_1}s_1 + \sqrt{P_2}s_2\right] + n_1, \tag{13}$$

$$r_2 = \sqrt{A_2}\left[\sqrt{P_1}s_1 + \sqrt{P_2}s_2\right] + n_2. \tag{14}$$

3 SOP and SPCS

Weak user detects its symbol s_1 with Signal to Interference plus Noise Ratio (SINR) given by

$$\gamma_2 = \frac{P_2 A_2}{P_1 A_2 + N_0}. \tag{15}$$

Strong user U_1 demodulates s_2 since it is transmitted with a larger power. The SINR at U_1 to detect s_2 is equal to

$$\gamma_{1\to 2} = \frac{P_2 A_1}{P_1 A_1 + N_0}. \tag{16}$$

Then, strong user removes s_1 and detects s_2 with SINR

$$\gamma_{1\to 1} = \frac{P_1 A_1}{N_0}. \tag{17}$$

The SINR at U_1 is the minimum of $\gamma_{1\to 1}$ and $\gamma_{1\to 2}$

$$\gamma_1 = min\left(\gamma_{1\to 1}, \gamma_{1\to 2}\right) \tag{18}$$

The outage probability at U_2 is expressed as

$$P^{outage,2}\left(\gamma_{th}\right) = P_{\gamma_2}\left(\gamma_{th}\right) = P_{A_2}\left(\frac{N_0\gamma_{th}}{P_2 - P_1\gamma_{th}}\right) \tag{19}$$

where $P_{A_2}(x)$ is the Cumulative Distribution Function of A_2 given by

$$P_{A_2}(x) = P\left(A_2 \le x\right) = P\left(-\sqrt{\frac{x}{2E_s\beta\beta_2}} \le W_2 \le \sqrt{\frac{x}{2E_s\beta\beta_2}}\right) \tag{20}$$

Using the Central Limit Theorem (CLT), we approximate A_i by a Gaussian r.v. with mean $m_{W_i} = \frac{N_i\pi}{4}$ and variance $\sigma^2_{W_i} = N_i(1 - \frac{\pi^2}{16})$ [1].

Therefore, we have

$$P_{A_2}(x) \simeq 0.5erfc\left(\frac{-\sqrt{\frac{N_0 x}{2E_s\beta\beta_2}} - m_{W_2}}{\sqrt{2}\sigma_{W_2}}\right) - 0.5erfc\left(\frac{\sqrt{\frac{N_0 x}{2E_s\beta\beta_2}} - m_{W_2}}{\sqrt{2}\sigma_{W_2}}\right) \tag{21}$$

There is no outage at user U_1 when SINRs $\gamma_{1\to 1}$ and $\gamma_{1\to 2}$ are larger than γ_{th}

$$\begin{aligned} P^{outage,1}\left(\gamma_{th}\right) &= P_{\gamma_1}\left(\gamma_{th}\right) = 1 - P\left(\gamma_{1\to 1} > \gamma_{th}, \gamma_{1\to 2} > \gamma_{th}\right) \\ &= P_{A_1}\left(max\left[\frac{N_0\gamma_{th}}{P_2 - P_1\gamma_{th}}, \frac{N_0\gamma_{th}}{P_1}\right]\right), \end{aligned} \tag{22}$$

where $P_{A_1}(x)$ is the CDF of A_1 equal to

$$\begin{aligned} P_{A_1}(x) \simeq\ & 0.5erfc\left(\frac{-\sqrt{\frac{N_0 x}{2E_s\beta\beta_1}} - m_{W_1}}{\sqrt{2}\sigma_{W_1}}\right) \\ & - 0.5erfc\left(\frac{\sqrt{\frac{N_0 x}{2E_s\beta\beta_1}} - m_{W_1}}{\sqrt{2}\sigma_{W_1}}\right) \end{aligned} \tag{23}$$

Let γ_E be the SNR at Eavesdropper expressed as

$$\gamma_E = E_S\beta_E\frac{|t|^2}{N_0} \tag{24}$$

For Rayleigh channels, γ_E is exponentially distributed with PDF expressed as [21]

$$p_{\gamma_E}(x) = \frac{N_0 e^{-\frac{xN_0}{E_S \beta_E}}}{E_S \beta_E} \tag{25}$$

The secrecy capacity of the user U_1 is expressed as

$$C_1 = 0.5ln\left(\frac{1+\gamma_1}{1+\gamma_E}\right) \tag{26}$$

where γ_1 is the SINR of user U_1 given in (16-18).

The Secrecy Outage Probability (SOP) of user U_1 is computed as

$$\begin{aligned} SOP &= P\big(C_1 < R_1\big) = P\left(0.5ln\left(\frac{1+\gamma_1}{1+\gamma_E}\right) < R_1\right) \\ &= P\big(1+\gamma_1 < \big[1+\gamma_E\big]e^{2R_1}\big). \end{aligned} \tag{27}$$

where R_1 is the transmission rate of U_1.

We deduce the SOP as follows

$$\begin{aligned} SOP_1 &= \int_0^{+\infty} P\big(\gamma_1 < [1+x]e^{2R_1} - 1\big) p_{\gamma_E}(x)dx \\ &= \int_0^{+\infty} P_{\gamma_1}\big((1+x)e^{2R} - 1\big) p_{\gamma_E}(x)dx. \end{aligned} \tag{28}$$

where $P_{\gamma_1}(x)$ is the CDF of SNR at U_1 given in (22) while $p_{\gamma_E}(x)$ is the PDF of SNR at eavesdropper given in (25).

The Probability of Strictly Positive Secrecy Capacity (SPSC) of user U_1 is computed as

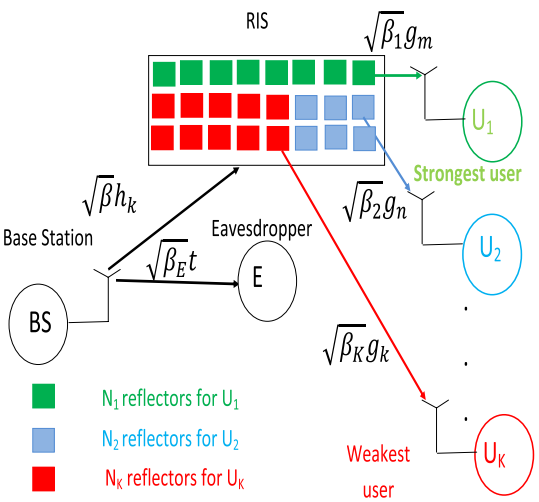

Fig. 2 NOMA with K users using reconfigurable intelligent surfaces (RIS)

$$\begin{aligned} SPSC_1 &= P(C_1 > 0) = P\big(\gamma_1 > \gamma_E\big) \\ &= \int_0^{+\infty} P\big(\gamma_1 \geq x\big) p_{\gamma_E}(x) dx \\ &= \int_0^{+\infty} \big[1 - P_{\gamma_1}(x)\big] p_{\gamma_E}(x) dx \end{aligned} \tag{29}$$

The secrecy capacity of user U_2 is expressed as

$$C_2 = 0.5 ln\left(\frac{1+\gamma_2}{1+\gamma_E}\right) \tag{30}$$

where γ_2 is the SINR at user U_2 given in (15).

Similarly, the SOP of user U_2 is computed as follows

$$\begin{aligned} SOP_2 &= \int_0^{+\infty} P\big(\gamma_2 < [1+x]e^{2R_2} - 1\big) p_{\gamma_E}(x) dx \\ &= \int_0^{+\infty} P_{\gamma_2}\big((1+x)e^{2R_2} - 1\big) p_{\gamma_E}(x) dx. \end{aligned} \tag{31}$$

where R_2 is the rate of user U_2, $P_{\gamma_2}(x)$ is the CDF of SNR at U_1 given in (19) while $p_{\gamma_E}(x)$ is the PDF of SNR at eavesdropper given in (25).

The Probability of Strictly Positive Secrecy Capacity (SPSC) of user U_2 is computed as

$$\begin{aligned} SPSC_2 &= P\big(C_2 > 0\big) = P\big(\gamma_1 > \gamma_E\big) \\ &= \int_0^{+\infty} \big[1 - P_{\gamma_2}(x)\big] p_{\gamma_E}(x) dx \end{aligned} \tag{32}$$

4 NOMA with Multiple Users Using RIS

Figure 2 shows the network model with K NOMA users. N_i reflectors of RIS refelect signals to user U_i. The total number of RIS reflectors is $N = \sum_{i=1} N_i$. I_i is the set of reflectors dedicated to user U_i. The BS transmits a linear combination of K symbols $s_1, s_2, ..., s_K$ to K users:

$$s = \sum_{i=1}^{K} \sqrt{P_i} s_i, \tag{33}$$

where $\sum_{i=1}^{K} P_i = 1$ and $0 < P_1 < P_2 < ... < P_K < 1$ are powers allocated to users U_1, U_2 ,...U_K.

The received signal at U_i is equal to

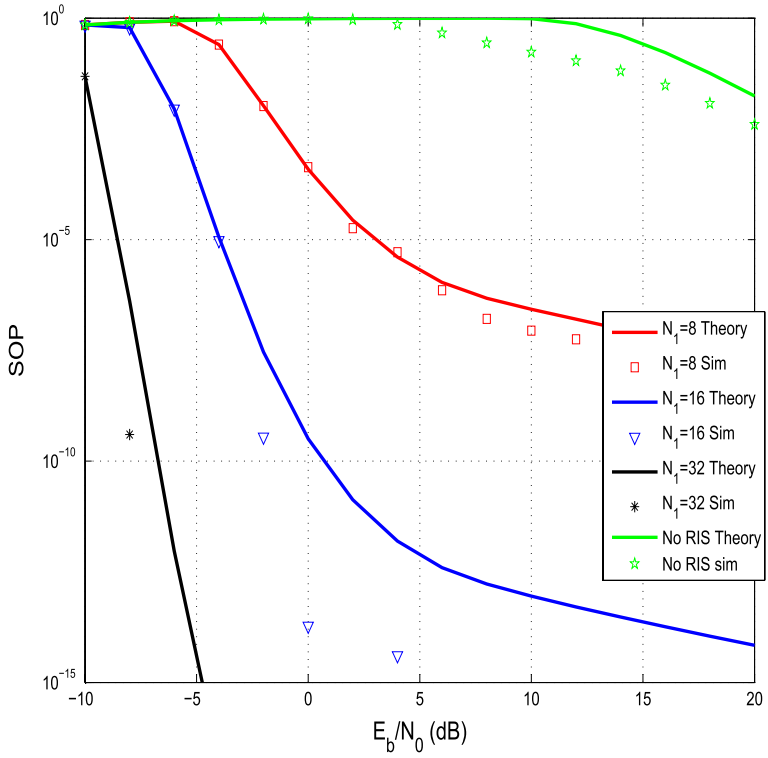

Fig. 3 SOP of strong user: NOMA with two users

$$r_i = s\sqrt{KE_s\beta\beta_1}\sum_{k\in I_i} a_k c_k + n_i, \tag{34}$$

We deduce

$$r_i = s\sqrt{A_i} + n_i, \tag{35}$$

where

$$A_i = KE_s\beta\beta_2 W_i^2, \tag{36}$$

$$W_i = \sum_{k\in I_i} a_k c_k, \tag{37}$$

U_i detects s_K since $P_K > P_{K-1} > ... > P_i$. The SINR at U_i to detect s_K is expressed as

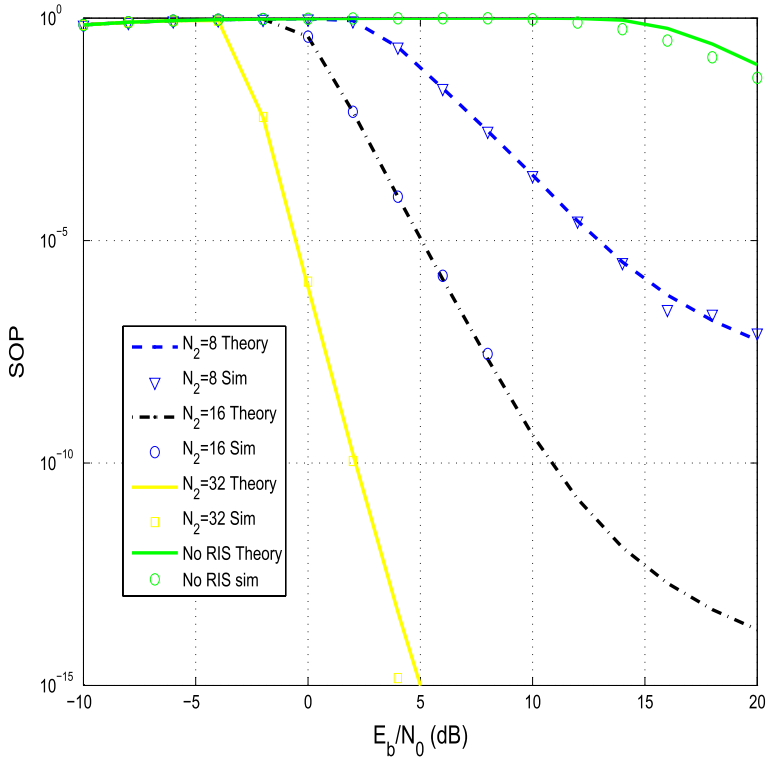

Fig. 4 SOP of weak user: NOMA with two users

$$\gamma_{i\to K} = \frac{A_i P_K}{N_0 + A_i \sum_{j=1}^{K-1} P_j} \tag{38}$$

U_i removes the contribution of s_K and detects s_{K-1} with SINR

$$\gamma_{i\to K-1} = \frac{A_i P_{K-1}}{N_0 + A_i \sum_{j=1}^{K-2} P_j} \tag{39}$$

The process is continued until U_i detects s_i. The SINR at U_i to detect s_q, $i \le q \le K$, is expressed as

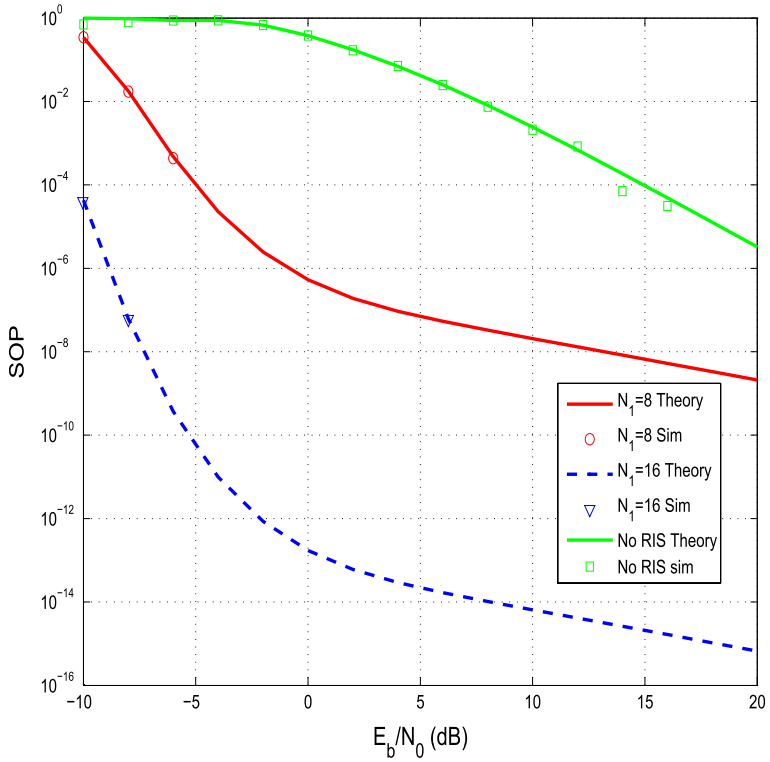

Fig. 5 SOP of strongest user: NOMA with three users

$$\gamma_{i\to q} = \frac{A_i P_q}{N_0 + A_i \sum_{j=1}^{q-1} P_j}, i \le q \le K, \tag{40}$$

There is no outage at U_i if SINRs $\gamma_{i\to K}, \gamma_{i\to K-1}, ..., \gamma_{i\to i}$ are greater than γ_{th}. The SINR at U_i is equal to

$$\gamma_i = min\left[\gamma_{i\to K}, \gamma_{i\to K-1}, ..., \gamma_{i\to i}\right] \tag{41}$$

We deduce the outage probability at U_i

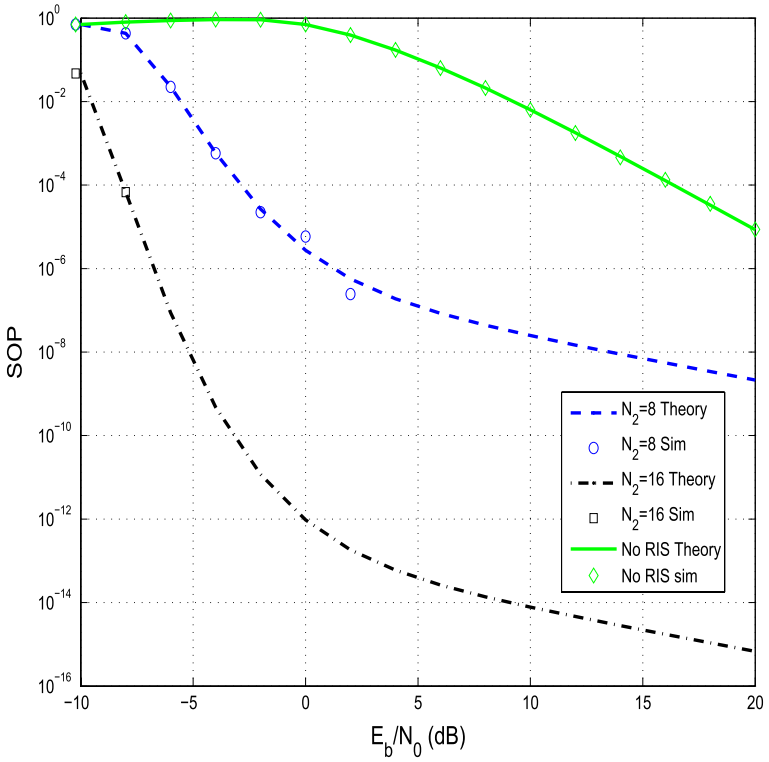

Fig. 6 SOP of middle user; NOMA with three users

$$
\begin{aligned}
P^{outage,i}(\gamma_{th}) &= P_{\gamma_i}(\gamma_{th}) \\
&= 1 - P\left(\gamma_{i\to K} > \gamma_{th}, \gamma_{i\to K-1} > \gamma_{th}, ..., \gamma_{i\to i} > \gamma_{th}\right) \\
&= P_{A_i}\left(\max_{i\le q\le K}\left(\frac{N_0\gamma_{th}}{P_q - \gamma_{th}\sum_{j=1}^{q-1} P_j}\right)\right),
\end{aligned}
\tag{42}
$$

where

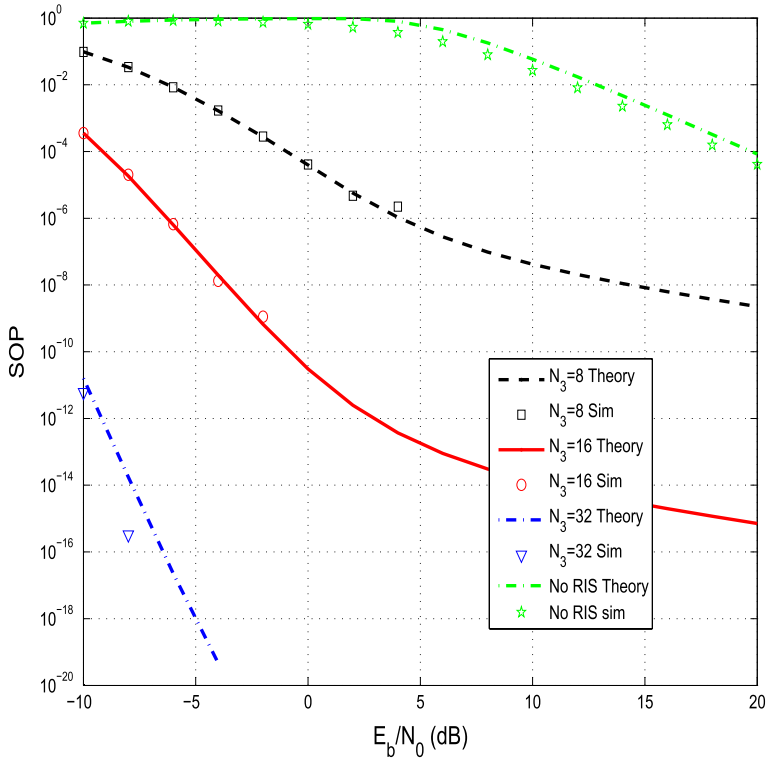

Fig. 7 SOP of weak user : NOMA with three users

$$P_{A_i}(x) \simeq 0.5 erfc\left(\frac{-\sqrt{\frac{N_0 x}{KE_s\beta\beta_i}} - m_{W_i}}{\sqrt{2}\sigma_{W_i}}\right) - 0.5 erfc\left(\frac{\sqrt{\frac{N_0 x}{KE_s\beta\beta_i}} - m_{W_i}}{\sqrt{2}\sigma_{W_i}}\right) \tag{43}$$

The secrecy capacity of the user U_i is expressed as

$$C_i = 0.5 ln\left(\frac{1+\gamma_i}{1+\gamma_E}\right) \tag{44}$$

where γ_i is the SINR at user U_i defined as the minimum of SINRs of all detected symbols:

$$\gamma_i = min\left[\gamma_{i\to K}, \gamma_{i\to K-1}, ..., \gamma_{i\to i}\right] \tag{45}$$

Similarly, the SOP of user U_i is computed as follows

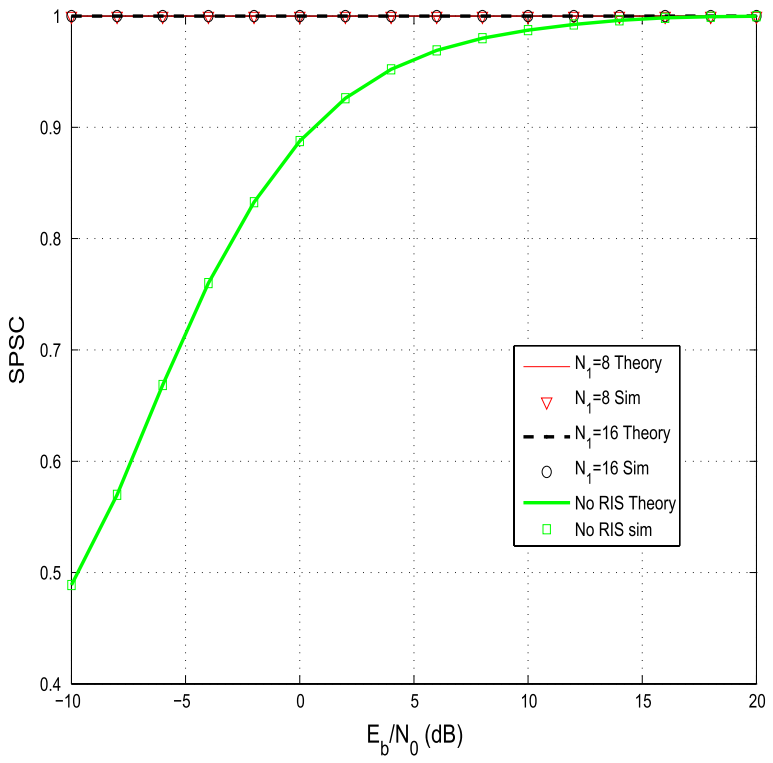

Fig. 8 SPSC of strong user : NOMA with two users

$$SOP_i = \int_0^{+\infty} P_{\gamma_i}\big((1+x)e^{2R_i} - 1\big) p_{\gamma_E}(x)dx. \tag{46}$$

where R_i is the rate of user U_i, $P_{\gamma_i}(x)$ is the CDF of SNR at U_i given in (42-43) while $p_{\gamma_E}(x)$ is the PDF of SNR at eavesdropper given in (25).

The Probability of Strictly Positive Secrecy Capacity (SPSC) is computed as

$$SPSC_i = \int_0^{+\infty} \big[1 - P_{\gamma_i}(x)\big] p_{\gamma_E}(x)dx \tag{47}$$

5 Theoretical and Simulation Results

Figures 3 and 4 depict the SOP at strong and weak users when there are two NOMA users. The distances are $d_1 = 1$, $d_2 = 1.5$ and $d_E = 3$. The path loss exponent is three. We observe that the proposed RIS offers 22, 28 and 34 dB gain with respect to conventional NOMA without RIS for a number of reflectors $N_1 = N_2 = 8, 16, 32$. We notice a good accordance between theoretical and simulation results.

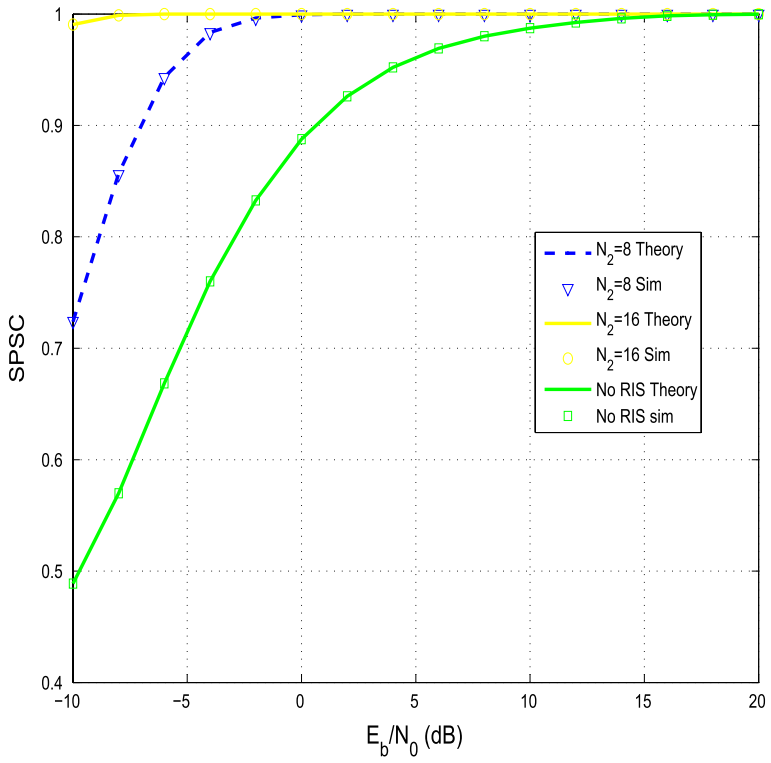

Fig. 9 SPSC of weak user : NOMA with two users

Figures 5, 6 and 7 depict the SOP at three NOMA users located at $d_1 = 0.8$, $d_2 = 1$ and $d_3 = 1.5$. The Eavesdropper is located at $d_E = 3$. We observe a significant enhancement on the physical layer security of NOMA using RIS. RIS offers 20, 30 dB gain with respect to conventional NOMA without RIS for a number of reflectors $N_1 = N_2 = N_3 = 8, 16$.

Figures 8and 9 depict the SPSC for NOMA with and without RIS when there are two users. The distances are $d_1 = 1$, $d_2 = 1.5$ and $d_E = 3$. We notice that RIS improves the physical layer security of NOMA systems.

6 Comparison with Current Literature

The main contribution of the paper is to improve the physical layer security of NOMA systems using RIS. We derived both the Secrecy Outage Probability (SOP) and the Strictly Positive Secrecy Capacity (SPSC) of NOMA using RIS. When there are two users, the proposed RIS improves the physical layer security by 22, 28 and 34 dB with respect to conventional NOMA without RIS [11, 12] for a number of reflectors $N_1 = N_2 = 8, 16, 32$. When there are three users, RIS offers 20, 30 dB gain with respect to conventional NOMA without RIS [11, 12] for a number of reflectors $N_1 = N_2 = N_3 = 8, 16$ per user.

7 Conclusions

In this paper, we improved the physical layer security of NOMA systems using Reconfigurable Intelligent Surfaces (RIS). When RIS is employed, the base station can reduce its power since all reflected signals have the phase phase at different NOMA users. We have compared the SOP and SPSC of NOMA systems when RIS is deployed to conventional NOMA without RIS. We have shown that the use of RIS improve the security of NOMA systems by 20-30 dB with respect to conventional wireless systems without RIS [10–13].

Acknowledgements This publication was supported by the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia.

Author Contributions The paper is the contribution of Prof. Faisal Alanazi.

Funding This publication received no funding.

Availability of Data Material Data and material are not available.

Declarations

Conflict of interest The authors state that there is no conflict of interest for this paper.

References

1. Basar, E., Di Renzo, M., De Rosny, J., Debbah, M., , Alouini, M. -S. & Zhang, R. (2019). Wireless communications through reconfigurable intelligent surfaces. *IEEE Access, 7*, 116753–116773.
2. Zhang, H., Di, B., Song, L., & Han, Z. (2020). Reconfigurable intelligent surfaces assisted communications with limited phase shifts: How many phase shifts are enough? *IEEE Transactions on Vehicular Technology, 69*(4), 4498–4502.
3. Di Renzo, M. (2019). 6G Wireless: Wireless networks empowered by reconfigurable intelligent surfaces. In *2019 25th Asia-Pacific Conference on Communications (APCC)*.
4. Basar, E. (2020). Reconfigurable intelligent surface-based index modulation: A new beyond MIMO paradigm for 6G.*IEEE Transactions on Communications, 68*(5), 3187–3196.
5. Qingqing, W., & Zhang, R. (2020). Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. *IEEE Communications Magazine, 58*(1), 106–112.
6. Huang, C., Zappone, A., Alexandropoulos, G. C., Debbah, M., & Yuen, C. (2019). Reconfigurable intelligent surfaces for energy efficiency in wireless communication. *IEEE Transactions on Wireless Communications, 18*(8), 4157–4170.
7. Alexandropoulos, G. C., & Vlachos, E. (2020). A hardware architecture for reconfigurable intelligent surfaces with minimal active elements for explicit channel estimation. In *ICASSP 2020—2020 IEEE international conference on acoustics, speech and signal processing (ICASSP)*.
8. Fang, D., Qian, Y., & Hu, R. Q. (2018). Security for 5G mobile wireless networks. *IEEE Access, 6,* 4850–4874.
9. Bloch, M., & Barros, J. (2011). *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge: Cambridge University Press.
10. Zhang, Y., Wang, H.-M., Yang, Q., et al. (2016). Secrecy sum rate maximization in non-orthogonal multiple access. *IEEE Communications Letters, 20*(5), 930–933.
11. Qin, Z., Liu, Y., & Ding, Z., et al. (2016). Physical layer security for 5G non-orthogonal multiple access in large-scale networks. In *Communications (ICC), 2016 IEEE International Conference on* (pp. 1-6). IEEE.
12. Liu, Y., Qin, Z., Elkashlan, M., et al. (2017). Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Transactions on Wireless Communications, 16*(3), 1656–1672.

13. Thapar, S., Mishra, D., & Saini, R. (2020). Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users. *IEEE Transactions on Vehicular Technology, 69*(11), 13259–13272.
14. Webb, H., Yin, C., Ngoc Nguyen, D., Le, T. T. N., Do, H. V., Van Hoang, D., & Van Nguyen, N. (2020). Secrecy outage analysis in energy harvesting relay networks with a friendly jammer. In *2020 4th international conference on recent advances in signal processing, telecommunications and computing (SigTelCom)*.
15. Dang-Ngoc, H.,Ho-Quoc, B., & Ho-Van, K. (2020). Key secrecy performance metrics of overlay networks with energy scavenging and artificial noise. In *2020 4th international conference on recent advances in signal processing, telecommunications and computing (SigTelCom)*.
16. Trinh, P. V., Carrasco-Casado, A. , Pham, A. T., & Toyoshima, M. (2020). Secrecy analysis of FSO systems considering misalignments and eavesdropper's location. *IEEE Transactions on Communications*.
17. Byungha, Y., In-Ho, L., & Haejoon, J. (2020). Exact secrecy rate analysis of antenna subset modulation schemes. *IEEE Systems Journal, Year, 68*(12), 7810–7823.
18. Kumar, S, Garg, A., & Bhatnagar, M. R. (2020). Physical layer secrecy performance analysis of imperfect feedback based 41 MISO system. In *2020 international conference on signal processing and communications (SPCOM)*.
19. He, B., Lv, L., Yang, L., & Chen, J. (2020). Enhancing secrecy for NOMA untrusted relay networks with user scheduling and jamming. *IEEE Communications Letters, 24*(12), 2682–2686.
20. Khojastehnia, M., & Loyka, S. (2020). Comments on 'Precoding for secrecy rate maximisation in cognitive MIMO wiretap channels'. *Electronics Letters, 56*(17), 902–904.
21. Proakis, J. (2007). *Digital Communications* (5th ed.). New-York: Mac Graw-Hill.

Faisal Alanazi (S'16-M'18) received his B.Sc. in Electrical Engineering-Communication & Electronics from KSU in 2010, and M.Sc. & Ph.D. degrees in Electrical & Computer Engineering from The Ohio State University in 2013, and 2018, respectively. He is currently working as Assistant Professor at the PSAU. His research interests span Cryptography, Vehicular Ad-Hoc Networks, Delay Tolerant Networks. He is a member of the IEEE Communication Society.