Received February 12, 2021, accepted March 2, 2021, date of publication March 12, 2021, date of current version March 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3065760

Impact of Residual Hardware Impairment on the IoT Secrecy Performance of RIS-Assisted NOMA Networks

QIN CHEN[1], MEILING LI[1], XIAOXIA YANG[1], RYAN ALTURKI[2], MOHAMMAD DAHMAN ALSHEHRI[3], AND FAZLULLAH KHAN[4], (Senior Member, IEEE)

[1]School of Electronics Information Engineering, Taiyuan University of Science and Technology, Taiyuan 030024, China
[2]Department of Information Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 24372, Saudi Arabia
[3]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[4]Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan

Corresponding author: Meiling Li (meilingli@tyust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62001320, in part by the Key Research and Development Program of Shanxi under Grant 201903D121117, in part by the Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi under Grant 201802090, in part by the Research Project Supported by Shanxi Scholarship Council of China under Grant 2020-126, in part by the Graduate Education Innovation Project of Shanxi under Grant 2020SY419, and in part by the Taif University Researchers Supporting Project under Grant TURSP-2020/126.

ABSTRACT Non-orthogonal multiple access (NOMA) technology is expected to effectively improve the spectrum efficiency of fifth-generation and later wireless networks. As a new technology, reconfigurable Intelligent surfaces (RIS) can achieve high spectral and energy efficiency with a low cost in wireless networks. These are achieved by integrating a great quantity of low-cost passive reflective units (RUs) on the plane. In this article, in order to meet the needs of high efficiency, low power consumption, and wide coverage, we combine RIS-assisted NOMA technology with the internet of things (IoT). Because in the actual wireless communication system, the residual hardware impairment (RHI) characteristics of the actual transceiver equipment will have an important impact on system secrecy performance. Therefore, the study will propose a single eavesdropper RIS-assisted downlink NOMA system with RHI (E-RHI-RIS-NOMA). The study will also investigate the impact of RHI on the physical layer security (PLS) performance of the system and the closed-form expression of the user's secrecy outage probability (SOP) is derived. Finally, the simulation results show that 1) the main factors affecting the SOP are the quantity of RUs in RIS, the transmit SNR, and the target data rate, 2) it is proved that the hardware impairment of the transceiver harms the system's secrecy outage performance while the severity of the impact of RHI on the system performance depends on the transmit SNR and target data rate. Moreover, RHI at different nodes has a different influence on system secrecy performance. 3) the system performance of RIS relying on NOMA is improved compared with orthogonal multiple access (OMA) and conventional NOMA.

INDEX TERMS Non-orthogonal multiple access, physical layer security, residual hardware impairment, secrecy outage probability, reconfigurable intelligent surface, Internet of Things.

I. INTRODUCTION

Internet of Things (IoT) technology is getting a lot of attention because of its huge potential to connect billions of devices in numerous applications [1]. Driven by economic and environmental concerns, and the scale of the next-generation IoT system, the design of energy-efficient high bandwidth wireless technology is becoming crucial [2].

Reconfigurable intelligent surfaces (RIS) are a revolutionizing technology in the field of wireless communication, which can adjust the wireless environment to improve spectrum and energy efficiency. It is considerd to be a extraordinary prospect and valid green resolve scheme in the next wireless communication [3]–[5]. RIS are artificial surfaces of electromagnetic materials controlled by integrated electronic devices with unique wireless communication capabilities. The intelligent radio environment is a kind of wireless network that transforms wireless network environment into

The associate editor coordinating the review of this manuscript and approving it for publication was Donghyun Kim.

reconfigurable intelligent space, which is controlled by telecom operators and plays a positive role in information transmission and processing [6]. Compared with current technologies, RIS achieve deterministic and programmable control of wireless environment behavior [7]. Most RIS implementations compose two dimension (2D) metasurfaces (MS) arrays.By tune-up the phase shift of each element skillfully, the propagation characteristics of the signal can be changed [8]. RIS can achieve lower energy consumption compared with communication auxiliary technology similar to amplifying and forwarding relays [5]. The RIS can be easily embedded into the interior of buildings and onto the surface of large vehicles not need to change the hardware and software of the device, making IoT performance improvements in connectivity, power, and coverage significantly less costly [9], [10]. Meanwhile, RIS can achieve a large range of coverage under low power consumption [1].

In the mass open heterogeneous access environment, IoT security is seriously challenged [11]. In wireless networks such as the IoT, communication security and secret protection are very significant, because the electromagnetic transmission has the nature of broadcasting, which makes the communication of the IoT vulnerable to eavesdropping attacks [12]. Traditional security methods are mainly based on authentication and cryptography, which are implemented in the upper layer of a wireless communication system but are relatively independent of the physical layer. However, for the traditional encryption technology, key management is difficult [13]. Physical layer security (PLS) technology from the perspective of information theory, makes use of the indeterminacy and time-variability of the wireless channel to realize the secure communication of encrypted link without key [14] and developed a promising solution for secure IoT communication. The PLS performance of downlink multi-user orthogonal frequency division multiplexing (OFDM) and uplink non-orthogonal multiple access (NOMA) IoT systems is studied in [15] and [16] respectively. In [17], to enhance the safety of the downlink multi-carrier IoT communication system with eavesdroppers, an effective PLS method is proposed.

Driven by the uniqueness of RIS, some preliminary studies have shown how to improve system secrecy performance through RIS. Reference [18] considered a RIS-assisted Gaussian multiple-input multiple-output (MIMO) eavesdropping channel, and an optimization algorithm is proposed maximized the secrecy rate of the channel. However, [19] studied the PLS issues of two vehicle-mounted system models using RIS-assisted transmission and [20] a single eavesdropping wireless communication system assisted by RIS is studied. By jointly designing AP transmission waveform and RIS reflection waveform, the confidentiality of legal communication link is improved to the maximum. The RIS propagate the incident electromagnetic wave to the target receiver in the expected way by changing the attenuation and scattering of the incident electromagnetic wave. Reference [21] proposed a multiple eavesdropper downlinks multiple-input single-output (MISO) system to improve system secrecy performance through RIS-assisted transmission. NOMA technology has been considered a promising candidate for multiple access in future mobile networks because of having high spectral efficiency, but also can guarantee the fairness of users, and can obtain powerful connection support [22], [23]. The core concept of NOMA is to use superimposed coding (SC) technology at the transmitter and successive interference cancellation (SIC) technology at the receiver to serve multiple users on the same time-frequency resource block [22]. NOMA enables IoT large-scale connection communication by increasing system throughput through the simultaneous transmission of multiple signals on the same resource block [24]. RIS provide a new method to enhance the performance of NOMA systems that is to reconstruct the wireless environment, which urges us to apply RIS technology to the NOMA system [25]. The influence of two distinct phase shift designs on the performance of RIS-assisted NOMA system was investigated by [26]. In the RIS-assisted NOMA system, [25] maximized the minimum decoding signal-to-noise ratio (SINR) by considering both the emission beam formation at BS and the phase shift at the RIS. Reference [5] considered the MISO-NOMA system, according to the characteristics of reflection amplitude and phase shift, assuming that RIS reflection exists in both ideal and non-ideal situations, a new algorithm is proposed to obtain the maximum total rate of all users.

All the aforementioned works assumed that the ideal situation of the transceiver. However, in actual communication systems, the transmitter and receiver hardware of wireless nodes are affected by non-ideal (RHI, Residual Hardware Impairment) characteristics frequently, such as I/Q imbalance, amplifier amplitude nonlinearity, and phase noise [27], [28]. Reference [29] investigated the effects of RHI and channel estimation errors(CEEs) on the security and reliability of multi-relay cooperative systems. References [30] and [31] considered a NOMA system with RHI and CEEs, and studied the outage probability of users under the system. The spectrum and energy efficiency of RIS-aided MISO system considering hardware impairment are analyzed and revealed the adverse effects of hardware impairment on system performance in [32]. Based on considering the hardware impairment, the energy efficiency is analyzed in the wireless communication system assisted by RIS [33]. According to the existing research work, the hardware impairment has seriously affected the performance of the wireless communication system with RIS-assisted transmission.

To the best of our knowledge, the secrecy performance of RIS-assisted NOMA system with non-ideal (RHI) hardware condition has not been investigated in the existing literature. Based on this motivation, this work investigates how the security performance of RIS-assisted NOMA system is affected by RHI. Specifically, the expressions of user secrecy outage probability (SOP) under non-ideal (RHI) hardware condition are derived, and the influence of user's SOP on system performance is analyzed. The numerical results show that the severity of RHI's impact on system performance is closely related to the SNR, target data rate, and power allocation coefficient, but it has nothing to do with the quantity of reflection units (RUs) in RIS. In this case of high SNR and high target data rate, RHI have a more significant influence on the secrecy performance of the system, and when the power allocation coefficient is taken at different values, the impact on system security performance also varies. Simulation result also shows RIS-assisted NOMA system compared with the traditional NOMA system and improvement in the secrecy performance, and the degree of performance improvement is related to the number of RIS's RUs. The key contributions of this article are follow.

- We provide a RIS-assisted downlink NOMA system with an eavesdropper. The model considers the impact of RHI on system secrecy performance.
- The SOP expression of RIS-assisted NOMA system is derived. These expressions can quantify the degradation of secrecy performance caused by RHI. How RHI and RIS's RUs affect the secrecy performance of the NOMA system is studied.
- Monte Carlo simulation studies the relationship between the severity of RHI impact on system performance and different parameters and provides useful insights into the impact of RHI on the SOP of the NOMA system.

The rest of this article is arranged as below: Section II describes the RIS-assisted NOMA system model, considering the influence of transceiver hardware imperfection. Section III takes the SOP as the performance index to evaluate the influence of the imperfect transceiver hardware on the performance of the RIS-assisted NOMA system. In Section IV, numerical results are given to prove the correctness of the analysis. Ultimately, the Section V is the conclusion.

II. SYSTEM MODEL

As shown in Fig 1, a downlink E-RHI-RIS-NOMA system is considered in this article, which consists of one base station(BS), one RIS, which consists of N RUs, two legitimate receivers (D_n, near the user, and D_m, far user), and one eavesdropper(*Eve*). BS communicates with two legitimate users at the same time and frequency through a RIS. Due to long-distance or major obstacles, we presume that there is no direct connection between the BS and the destination [34]. Furthermore, we assume that all nodes in the system have only one antenna. The channel coefficients of the BS to i-th RU, the i-th RU to destination D_κ ($\kappa \in \{n, m\}$) and the i-th RU to *Eve* are denoted by h_{si}, g_{id_κ} and g_{ie}, respectively. And all the channels follow independent Rayleigh fading.

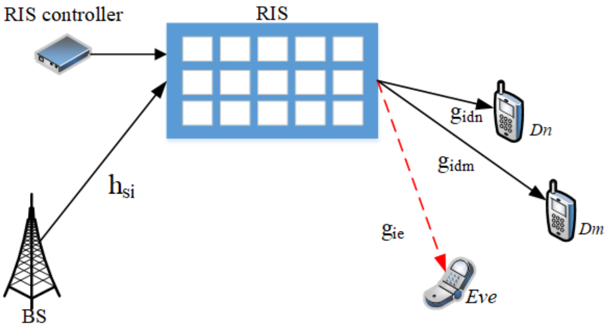

FIGURE 1. E-RHI-RIS-NOMA system model.

In the first phase, BS sends a superimposed mixed signal to RIS, assuming that the RF front end is not ideal, the transmission signal at BS is

$$x_S = \sqrt{\alpha_n P_S} x_n + \sqrt{\alpha_m P_S} x_m + \mu_S \tag{1}$$

where x_n is the message of the n-th user (i.e.,D_n), $E\left[|x_n|^2\right] = 1$, α_n denotes the power allocation coefficient of the n-th user and satisfying $\alpha_n < \alpha_m$ and $\alpha_n + \alpha_m = 1$. In this article, we consider that each node in the system has RHI. The impact of RHI can be used as additional noise source to model [35]. Thus, μ_S denotes the distortion caused by hardware impairment at the BS, $\mu_s \sim \mathcal{CN}\left(0, \left(\rho_S^t\right)^2 P_S\right)$, ρ_S^t stands for the BS's error vector magnitudes (EVMs). According to the 3rd generation partnership project (3GPP) long term evolution advanced (LTE-A), the minimum and maximum hardware impairments are 0.08 and 0.175, respectively [36]. P_S represents the average transmitted power at the BS.

In the second phase, RIS can play the part of repeater, forwarding information to the NOMA users. Therefore, the signals received by legitimate users under the existence of RHI is given by

$$y_{D_\kappa} = \sum_{i=1}^{N} h_{si} r_i g_{id_\kappa} \left(x_S + \mu_{D_\kappa}\right) + n_{D_\kappa} \tag{2}$$

where $\kappa \in \{n, m\}$, $r_i = \beta_i \exp(j\theta_i)$ is the response of the i-th RU, and the reflection coefficients of phase shift and amplitude of the i-th RU are represented by β_i and θ_i respectively. Without losing generality, we presume that $\beta_i = 1$. μ_{D_κ} is the distortion caused by a hardware impairment at the legitimate user D_κ, $\mu_{D_\kappa} \sim \mathcal{CN}\left(0, \left(\rho_{D_\kappa}^r\right)^2 P_S\right)$, n_{D_κ} stands for the additive white Gaussian noise (AWGN) and $n_{D_\kappa} \sim \mathcal{CN}\left(0, \sigma_{D_\kappa}^2\right)$. To facilitate the analysis, we assume that $\sigma_{D_\kappa}^2 = \sigma_D^2$.

On the other hand, when RIS-assisted transmitting information to the target user, the eavesdropper will intercept the corresponding information. Therefore, the signal received by the *Eve* can be given

$$y_E = \sum_{i=1}^{N} h_{si} r_i g_{ie} \left(x_S + \mu_E\right) + n_E \tag{3}$$

where μ_E represents the distortion caused by hardware impairment at the *Eve*, $\mu_E \sim \mathcal{CN}\left(0, \left(\rho_E^r\right)^2 P_S\right)$, n_E represents AWGN at the *Eve*, $n_E \sim \mathcal{CN}\left(0, \sigma_E^2\right)$.

We can achieve different phase shifts of RIS components independently by setting the corresponding set voltage with microcontroller [37]. We assume that RIS are completely aware of the phase θ_i of $BS \rightarrow RIS$ channel h_{si} and the phase ψ_i of $RIS \rightarrow D_\kappa/Eve$ channel g_{id} and g_{ie}, and choose the best phase shift, i.e.

$$\phi_i = -\left(\theta_i + \psi_i\right) \tag{4}$$

r_i can be further written as

$$r_i = \exp\left(-j\left(\theta_i + \psi_i\right)\right) \tag{5}$$

Next, by substituting (5) into (2) and (3), we can get [38]

$$y_{D_\kappa} = A_\kappa\left(x_S + \mu_{D_\kappa}\right) + n_{D_\kappa} \tag{6}$$

$$y_E = A_e\left(x_S + \mu_E\right) + n_E \tag{7}$$

where $A_\kappa = \sum\limits_{i=1}^{N} |h_{si}||g_{id_\kappa}|$, $A_e = \sum\limits_{i=1}^{N} |h_{si}|\,|g_{ie}|$.

Then by substituting (1) into (6) and (7), can be further expressed as

$$\begin{aligned} y_{D_\kappa} &= A_\kappa\left(\sqrt{\alpha_n P_S}x_n + \sqrt{\alpha_m P_S}x_m + \mu_S + \mu_{D_\kappa}\right) + n_{D_\kappa} \\ &= A_\kappa\left(\sqrt{\alpha_n P_S}x_n + \sqrt{\alpha_m P_S}x_m + \mu_{SD_\kappa}\right) + n_{D_\kappa} \end{aligned} \tag{8}$$

$$\begin{aligned} y_E &= A_e\left(\sqrt{\alpha_n P_S}x_n + \sqrt{\alpha_m P_S}x_m + \mu_S + \mu_E\right) + n_E \\ &= A_e\left(\sqrt{\alpha_n P_S}x_n + \sqrt{\alpha_m P_S}x_m + \mu_{SE}\right) + n_E \end{aligned} \tag{9}$$

where μ_{SD_κ} and μ_{SE} represent the RHI's aggregation distortion in the link $BS \rightarrow D_\kappa$ and $BS \rightarrow Eve$, respectively. $\mu_{SD_\kappa} \sim \mathcal{CN}\left(0, \rho^2_{SD_\kappa}P_s\right)$, $\rho^2_{SD_\kappa} = \left(\rho^t_S\right)^2 + \left(\rho^r_{D_\kappa}\right)^2$, $\mu_{SE} \sim \mathcal{CN}\left(0, \rho^2_{SE}P_s\right)$, $\rho^2_{SE} = \left(\rho^t_S\right)^2 + \left(\rho^r_E\right)^2$.

III. PERFORMANCE ANALYSIS

In the E-RHI-RIS-NOMA system model shown in Fig. 1, the influence of transceiver hardware impairment on system performance is quantified. This section is structured as follows: Section III-A gives the SIDNR. Section III-B analyzes the channel statistical characteristics, as the basis for the subsequent analysis of the secrecy outage performance. Finally, Section III-C provides the expressions of the SOP.

A. SIDNR

NOMA uses SIC receivers at the receiving end to realize multi-user detection (MUD). The basic principle of SIC is to gradually subtract the interference of users with the highest signal power, and operate in the order of signal power. Since in NOMA, users with poor channel state, larger power is allocated when transmitting information, so D_n first decodes the message of weaker D_m. Consequently, the signal interference plus distortion noise ratio (SIDNR) for D_n to detect x_m can be obtained from (8)

$$\gamma_{D_n \rightarrow D_m} = \frac{\alpha_m |A_n|^2}{|A_n|^2\left(\alpha_n + \rho^2_{SD_n}\right) + \frac{1}{\rho_S}} \tag{10}$$

where $\rho_S = \frac{P_S}{\sigma^2_D}$ average SNR of legal links, $A_n = \sum\limits_{i=1}^{N} |h_{si}||g_{id_n}|$ is the equivalent $BS - RIS - D_n$ channel.

And then D_n subtracts the D_m signal from the received signal, the received SIDNR at D_n to detect its own message is given by

$$\gamma_{D_n} = \frac{\alpha_n |A_n|^2}{|A_n|^2 \rho^2_{SD_n} + \frac{1}{\rho_S}} \tag{11}$$

When D_m decode its own message, the stronger D_n's signal x_n will be treated as noise, and the SIDNR can be expressed as from (8)

$$\gamma_{D_m} = \frac{\alpha_m |A_m|^2}{|A_m|^2\left(\alpha_n + \rho^2_{SD_m}\right) + \frac{1}{\rho_S}} \tag{12}$$

where $A_m = \sum\limits_{i=1}^{N} |h_{si}||g_{id_m}|$ is the equivalent $BS{-}RIS - D_m$ channel.

Similar to [39], we assume the worst case, that is the eavesdropper has strong detection capabilities, and can detect x_n(or x_m) without interference from x_m (or x_n). From (9), we can get the SIDNR when Eve intercepts information x_n and x_m, respectively.

$$\gamma_{E_n} = \frac{\alpha_n |A_e|^2}{|A_e|^2 \rho^2_{SE} + \frac{1}{\rho_E}} \tag{13}$$

$$\gamma_{E_m} = \frac{\alpha_m |A_e|^2}{|A_e|^2\left(\alpha_n + \rho^2_{SE}\right) + \frac{1}{\rho_E}} \tag{14}$$

where $\rho_E = \frac{P_S}{\sigma^2_E}$, $A_e = \sum\limits_{i=1}^{N} |h_{si}|\,|g_{ie}|$ is the equivalent $BS - RIS - Eve$ channel.

B. CHANNEL STATISTICAL CHARACTERISTICS

Based on the E-RHI-RIS-NOMA system model proposed in Fig 1, this section first analyzes the channel statistical characteristics of the composite variables involved in the article, as the basis for the subsequent analysis of the secrecy outage performance.

Theorem 1: According to (11) and (12), the cumulative distribution function (CDF) of the γ_{D_n} and γ_{D_m} are displayed at the bottom of the next page.

where $\gamma\left(\cdot,\cdot\right)$ and $\Gamma\left(\cdot\right)$ represent the lower incomplete Gamma function and Gamma function respectively.

Proof: Please see Appendix A.

Theorem 2: The probability density function (PDF) of the γ_{E_n} and γ_{E_m} are displayed at the bottom of the next page.

Proof: Please see Appendix B.

C. SECRECY OUTAGE PROBABILITY

The SOP of the E-RHI-RIS-NOMA system is analyzed in this section. The secrecy outage event is defined as when the user's secrecy rate is lower than a predetermined threshold, the secrecy outage happened. $C_\kappa = \left\lceil \log_2\left(1 + \gamma_{D_\kappa}\right) - \log_2\left(1 + \gamma_{E_\kappa}\right)\right\rceil^+$ represents the achievable secrecy rate of .Therefore, the SOP expression can be formulated as

$$
\begin{aligned}
SOP_{\kappa} &= P_r\left\{C_{\kappa} < R_{\kappa}\right\} \\
&= P_r\left\{\gamma_{D_{\kappa}} < 2^{R_{\kappa}}\left(1+\gamma_{E_{\kappa}}\right)-1\right\} \\
&= \int_0^{\infty} F_{\gamma_{D_{\kappa}}}\left(2^{R_{\kappa}}(1+y)-1\right) f_{\gamma_{E_{\kappa}}}(y)\, dy \qquad (19)
\end{aligned}
$$

where $\lceil x \rceil^{+} = \max\{x, 0\}$ [40], $\kappa = \{n, m\}$ and R_{κ} is the target data rate of the user κ.

In order to obtain the SOP of D_n and D_m respectively, we made the following analysis.

1) SOP$_n$ ANALYSIS

Combining the discussion of $F_{\gamma_{D_n}}(x)$ and $f_{\gamma_{E_n}}(y)$ in Theorem 1 and Theorem 2, SOP_n is given by

$$
\begin{aligned}
SOP_n = &\int_0^{\theta_n^*} F_{\gamma_{D_n}}\left(2^{R_n}(1+y)-1\right) f_{\gamma_{E_n}}(y)\, dy \\
&+]\, 1 - F_{\gamma_{E_n}}\left(\theta_n^*\right) \qquad (20)
\end{aligned}
$$

where $\theta_n^* = \min\left(\frac{\alpha_n}{\rho_{SE}^2}, \frac{\alpha_n+\rho_{SD_n}^2\left(1-2^{R_n}\right)}{2^{R_n}\rho_{SD_n}^2}\right)$.

Substituting (15) and (17) into (20), we can get the expression of SOP, finding the closed expression is a challenging task. Nevertheless, the approximate expression can be obtained by utilizing the Gaussian-Chebyshev Quadrature theorem [41]. We let $\Lambda_1(y) = F_{\gamma_{D_n}}\left(2^{R_n}(1+y)-1\right) f_{\gamma_{E_n}}(y)$, (20) can be further approximated as

$$
\begin{aligned}
SOP_n \approx &\sum_{v=1}^{V} \frac{\theta_n^*}{2}\frac{\pi}{V}\sqrt{1-\varphi_v^2}\,\Lambda_1\left(\frac{\theta_n^*}{2}\left(1+\varphi_v\right)\right) \\
&+ 1 - F_{\gamma_{E_n}}\left(\theta_n^*\right) \qquad (21)
\end{aligned}
$$

where $\varphi_v = \cos\left(\frac{2v-1}{2V}\pi\right)$.

2) SOP$_m$ ANALYSIS

Combining the discussion of $F_{\gamma_{D_m}}(x)$ and $f_{\gamma_{E_m}}(y)$ in Theorem 1 and Theorem 2, SOP_m is given by

$$
\begin{aligned}
SOP_m = &\int_0^{\theta_m^*} F_{\gamma_{D_m}}\left(2^{R_m}(1+y)-1\right) f_{\gamma_{E_m}}(y)\, dy \\
&+ 1 - F_{\gamma_{E_m}}\left(\theta_m^*\right) \qquad (22)
\end{aligned}
$$

where $\theta_m^* = \min\left(\frac{\alpha_m}{\alpha_n+\rho_{SE}^2}, \frac{\alpha_m+\left(\alpha_n+\rho_{SD_m}^2\right)\left(1-2^{R_m}\right)}{2^{R_m}\left(\alpha_n+\rho_{SD_m}^2\right)}\right)$.

Similar to the analysis of SOP_n, substituting (16) and (18) into (22), SOP_m can be approximately expressed as

$$
\begin{aligned}
SOP_m \approx &\sum_{v=1}^{V} \frac{\theta_m^*}{2}\frac{\pi}{V}\sqrt{1-\varphi_v^2}\,\Lambda_2\left(\frac{\theta_m^*}{2}\left(1+\varphi_v\right)\right) \\
&+ 1 - F_{\gamma_{E_m}}\left(\theta_m^*\right) \qquad (23)
\end{aligned}
$$

where $\Lambda_2(y_2) = F_{\gamma_{D_m}}\left(2^{R_m}(1+y_2)-1\right) f_{\gamma_{E_m}}(y_2)$.

$$
F_{\gamma_{D_n}}(x) = \begin{cases} \dfrac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\ \frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SD_n}^2 x}}\sqrt{\frac{x}{\rho_S}}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & x \le \dfrac{\alpha_n}{\rho_{SD_n}^2} \\ 1, & otherwise \end{cases} \qquad (15)
$$

$$
F_{\gamma_{D_m}}(x) = \begin{cases} \dfrac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\ \frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\left(\alpha_m-\left(\alpha_n+\rho_{SD_m}^2\right)x\right)}}\frac{x}{\rho_S}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & x \le \dfrac{\alpha_m}{\alpha_n+\rho_{SD_m}^2} \\ 1, & otherwise \end{cases} \qquad (16)
$$

$$
f_{\gamma_{E_n}}(y) = \begin{cases} \dfrac{\alpha_n\left(\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\right)^{\frac{\pi^2}{16-\pi^2}N+2}\left(\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\rho_E}}\right)^{\frac{\pi^2}{16-\pi^2}N}\left(\sqrt{y}\right)^{\frac{\pi^2}{16-\pi^2}N-2} e^{-\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\sqrt{\frac{y}{\rho_E}}}}{2\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & y \le \dfrac{\alpha_n}{\rho_{SE}^2} \\ 0, & otherwise \end{cases} \qquad (17)
$$

$$
f_{\gamma_{E_n}}(y) = \begin{cases} \dfrac{\alpha_n\left(\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\right)^{\frac{\pi^2}{16-\pi^2}N+2}\left(\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\rho_E}}\right)^{\frac{\pi^2}{16-\pi^2}N}\left(\sqrt{y}\right)^{\frac{\pi^2}{16-\pi^2}N-2} e^{-\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\sqrt{\frac{y}{\rho_E}}}}{2\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & y \le \dfrac{\alpha_n}{\rho_{SE}^2} \\ 0, & otherwise \end{cases} \qquad (18)
$$

IV. SIMULATION AND RESULTS

In this section, the performance of E-RHI-RIS-NOMA system is analyzed and verified by building Matlab simulation platform and compare them with the traditional NOMA system without RIS-assisted. Assuming that the channels gain follow Rayleigh distribution, and how would the system performance be affected by the RHI level and the quantity of RUs in RIS are investigated. In this section, unless otherwise specified, we assume that the power allocation coefficients $\alpha_n = 0.4$, $\alpha_m = 0.6$, when $\alpha_n \neq 0.4$, $\alpha_m = 1 - \alpha_n$; The target data rates R_n and R_m of D_n and D_m are 0.1 bps/Hz and 0.05 bps/Hz, respectively. At the same time, assuming that all nodes are affected by RHI and $\rho_s^t = \rho_{D_n}^r = \rho_{D_m}^r = \rho_E^r = \rho$.

As can be seen from Fig. 2, the SOP curves in Monte Carlo are very consistent with the analytical results of the mathematical derivation, which proves the correctness of our derivation. Moreover, we can find that for NOMA users D_n and D_m, the secrecy outage performance of D_n is significantly greater than that of D_m, and the performance gap between the two users becomes more obvious as the value of N increases.

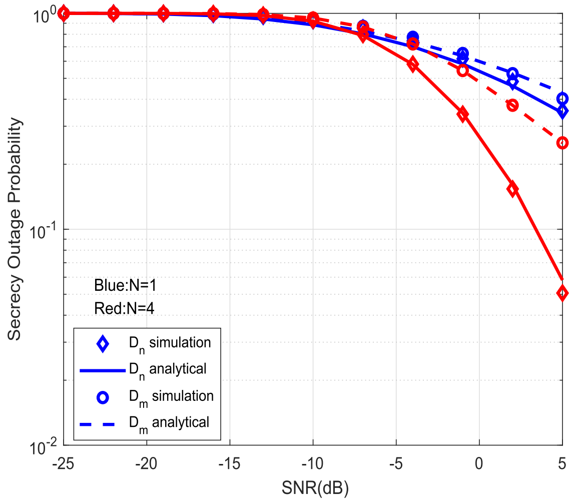

FIGURE 2. SOP of D_n and D_m.

The secrecy outage performance of RIS-assisted NOMA for near user D_n by comparing three different cases is shown in Fig 3. We observe that with the increase of ρ_S, the secrecy performance of NOMA system is improved. Therefore, the secrecy performance can be improved by enhancing the transmit SNR. In addition, the secrecy performance of the system is closely related to the target data rate. When N is fixed, the higher the target data rate is, the higher the SOP is. Furthermore, when R_n is a fixed value, system security performance is improved with the increase of RUs.

Fig. 4 describes the relationship between the SOP and the ρ_S at different target data rates and RHI levels when $N = 3$. As a benchmark, we simulated the SOP under ideal conditions, that is the situation where $\rho = 0$. Fig. 4 shows that with the increase of ρ, the user's secrecy performance decreases. For example, when taking $\rho_S = 1dB$ and $R_n = 0.5bps/Hz$, the value of ρ increases from 0 to 0.15, and the SOP increased from 5×10^{-1} to 6×10^{-1}. Meanwhile, we observe that the influence of RHI on the security performance of the system increased with the increase of the target data rate.

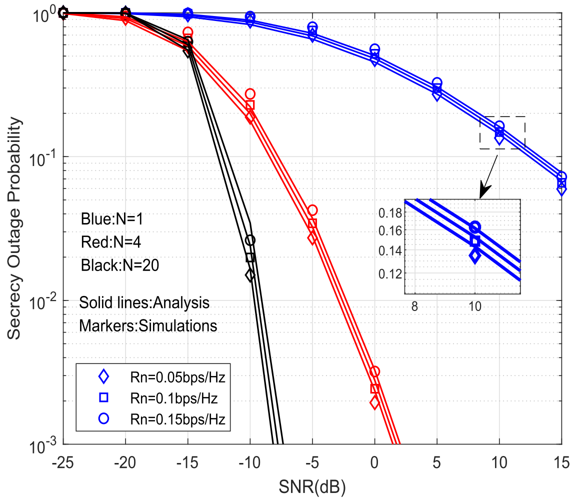

FIGURE 3. SOP varies with ρ_S under different R_n and N, $\rho = 0.1$.

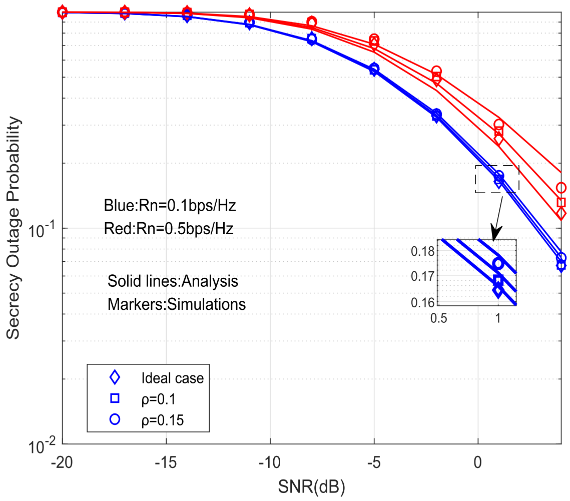

FIGURE 4. SOP varies with ρ_S under different ρ and R_n, $N = 3$.

In Fig. 5, we can see the effect of RHI on the performance of secrecy outage when ρ and N are different. To compare the influence of RHI on the SOP, we draw the curve when $\rho = 0$ as a comparison. For the ideal situation, neither the transmitter nor the receiver will be affected by hardware impairments, and the best secrecy outage performance can be observed. As can be seen from Fig. 5, the presence of RHI will notably reduce the performance of secrecy outage of the E-RHI-RIS-NOMA system. In particular, we observe that when $N = 1$, ρ increases from 0 to 0.15, to achieve the same SOP, the ρ_S should be increased by about 2dB. As shown in Fig. 5, the secrecy outage performance of user D_n shows a similar trend when we change values of N.

Fig. 6 shows the variations of SOP for user D_n when RHI exists in different nodes. It can be seen that when RHI only

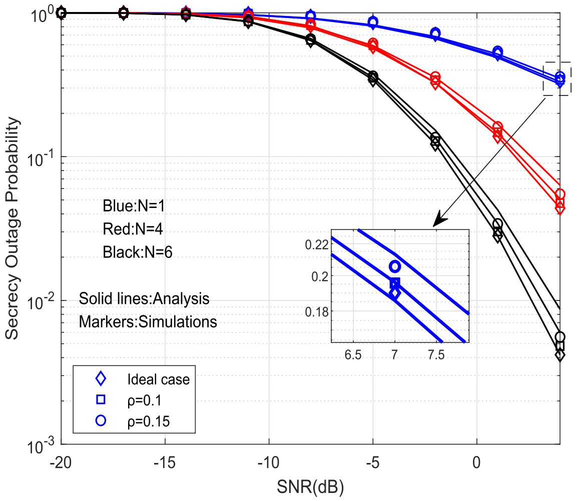

FIGURE 5. SOP varies with ρ_S under different values of ρ and N, $R_n = 0.1$.

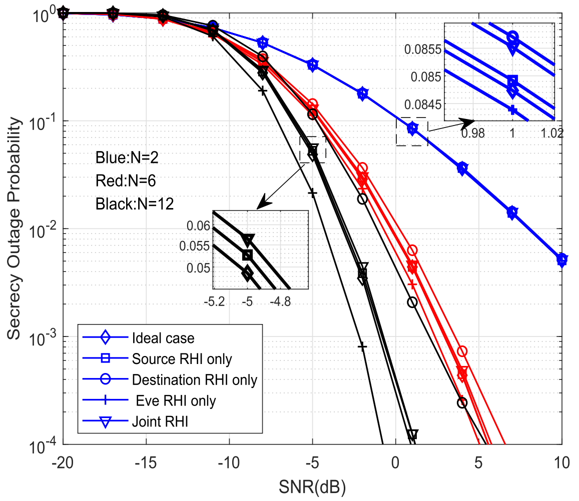

FIGURE 6. SOP varies with ρ_S when RHI at different nodes and different N, $R_n = 0.1$.

occurs in the destination node and eavesdropping node, it has a much bigger effect on the probability of secrecy outage, and the impact degree becomes more obvious with the increase of N. For example, taking $N = 12$, when the SOP is 1×10^{-2}, there will be about 1dB performance improvement and 2dB performance loss under the cases of RHI existing only in the eavesdropper node and in the destination node compared with the ideal hardware case, respectively. In addition, it can also be seen that the joint RHI not only affects the legitimate users but also aggravates the performance of eavesdropping users. The total secrecy performance loss caused by this is slightly less than that of RHI only occurred in the destination node.

As can be seen from Fig. 7, compared with RIS-assisted OMA and conventional NOMA systems, RIS-assisted NOMA system has more advantages in improving secrecy performance. With the increase of ρ_S, the performance advantage of RIS-assisted NOMA system is more obvious. And the higher the N value, the better the secrecy performance obtained for the RIS-assisted NOMA system. Therefore, the secrecy performance of the NOMA system can be effectively improved by deploying RIS reasonably.

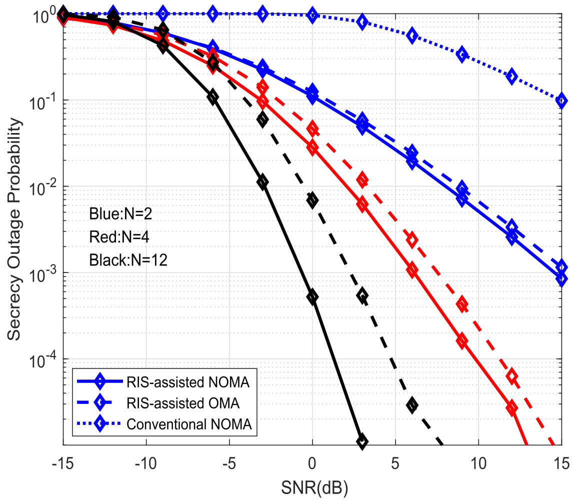

FIGURE 7. SOP of RIS-assisted NOMA contrasted with RIS-assisted OMA and conventional NOMA, $\rho = 0.1$.

V. CONCLUSION

In this article, the impacts of RHI on the secrecy outage performance under Rayleigh fading conditions of the proposed E-RHI-RIS-NOMA system model are investigated. In particular, in order to evaluate the secrecy performance when the transceiver hardware is imperfection, an approximate closed-form expression for the probability of secrecy outage is derived. The simulation results show that the main factors affecting the SOP are the quantity of RUs in RIS, the transmit SNR, and the target data rate. Throughout simulations, it is proved that the secrecy outage performance of the system will be adversely affected by the hardware impairment of the transceiver, and the severity of the impact of RHI on the system performance depends on the transmit SNR, target data rate. Moreover, RHI at different nodes has a different influence on system secrecy performance. In addition, the simulation results show that compared to the RIS-assisted OMA system and the conventional NOMA system, the RIS-assisted NOMA system has greater advantage in terms of secrecy performance. This finding is helpful for the design of RIS in the actual system and satisfy a large number of connections.

APPENDIX A PROOF OF THEOREM1

According to (10), we can get the cumulative distribution function (CDF) of γ_{D_n}

$$F_{\gamma_{D_n}}(x) = P_r\left\{|A_n|^2\left(\alpha_n - \rho_{SD_n}^2 x\right) \le \frac{x}{\rho_S}\right\} \quad \text{(A.1)}$$

$$f_{\gamma_{E_n}}(y)=\begin{cases}\dfrac{\alpha_n\left(\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\right)^{\frac{\pi^2}{16-\pi^2}N+2}\left(\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\rho_E}}\right)^{\frac{\pi^2}{16-\pi^2}N}\left(\sqrt{y}\right)^{\frac{\pi^2}{16-\pi^2}N-2}e^{-\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\sqrt{\frac{y}{\rho_E}}}}{2\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & y\le\dfrac{\alpha_n}{\rho_{SE}^2}\\ 0, & otherwise\end{cases}\tag{B.3}$$

$$f_{\gamma_{E_m}}(y)=\begin{cases}\dfrac{\alpha_m\left(\frac{1}{\sqrt{\alpha_m-\left(\alpha_n+\rho_{SE}^2\right)y}}\right)^{\frac{\pi^2}{16-\pi^2}N+2}\left(\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\rho_E}}\right)^{\frac{\pi^2}{16-\pi^2}N}\left(\sqrt{y}\right)^{\frac{\pi^2}{16-\pi^2}N-2}e^{-\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_m-\left(\alpha_n+\rho_{SE}^2\right)y}}\sqrt{\frac{y}{\rho_E}}}}{2\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}, & y\le\dfrac{\alpha_m}{\alpha_n+\rho_{SE}^2}\\ 0, & otherwise\end{cases}\tag{B.4}$$

for $\alpha_n-\rho_{SD_n}^2 x\ge 0$, or equivalently $x\le\frac{\alpha_n}{\rho_{SD_n}^2}$:

$$\begin{aligned}F_{\gamma_{D_n}}(x)&=P_r\left\{|A_n|^2\le\frac{x}{\rho_S\left(\alpha_n-\rho_{SD_n}^2 x\right)}\right\}\\&=P_r\left\{A_n\le\frac{1}{\sqrt{\left(\alpha_n-\rho_{SD_n}^2 x\right)}}\sqrt{\frac{x}{\rho_S}}\right\}\\&=F_{A_1}\left(\frac{1}{\sqrt{\left(\alpha_n-\rho_{SD_n}^2 x\right)}}\sqrt{\frac{x}{\rho_S}}\right)\end{aligned}\tag{A.2}$$

F_{A_n} is the CDF of A_n, $F_{A_n}(x)=\frac{\gamma\left(1+a,\frac{x}{b}\right)}{\Gamma(1+a)}$, where $a=\frac{k_1^2}{k_2}-1$, $b=\frac{k_2}{k_1}$, with $k_1=\frac{N\pi}{2}$ and $k_2=4N\left(1-\frac{\pi^2}{16}\right)$[34], the CDF of γ_{D_n} can be written as

$$F_{\gamma_{D_n}}(x)=\frac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SD_n}^2 x}}\sqrt{\frac{x}{\rho_S}}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}\tag{A.3}$$

According to (11), the CDF of γ_{D_m} is defined as

$$F_{\gamma_{D_m}}(x)=P_r\left\{|A_m|^2\left(\alpha_m-\left(\alpha_n+\rho_{SD_m}^2\right)x\right)\le\frac{x}{\rho_S}\right\}\tag{A.4}$$

Considering the condition of $x\le\frac{\alpha_m}{\alpha_n+\rho_{SD_m}^2}$, we have the same analysis process as (A.3), and we have the CDF of γ_{D_m} as

$$F_{\gamma_{D_m}}(x)=\frac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\left(\alpha_m-\left(\alpha_n+\rho_{SD_m}^2\right)x\right)}}\sqrt{\frac{x}{\rho_S}}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}\tag{A.5}$$

This completes the proof.

APPENDIX B PROOF OF THEOREM2

In order to calculate the probability density functions (PDFs) of γ_{E_n} and γ_{E_m}, we need to obtain their CDF firstly. The analysis process of the CDF is same as Appendix A. Therefore, according to (14) and (14), we recall the CDFs of γ_{E_n} and γ_{E_m} as below, and consider the conditions $y\le\frac{\alpha_n}{\rho_{SE}^2}$ and $y\le\frac{\alpha_m}{\alpha_n+\rho_{SE}^2}$ respectively

$$F_{\gamma_{E_n}}(y)=\frac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\alpha_n-\rho_{SE}^2 y}}\sqrt{\frac{y}{\rho_E}}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}\tag{B.1}$$

$$F_{\gamma_{E_m}}(y)=\frac{\gamma\left(\frac{\pi^2}{16-\pi^2}N,\frac{2\pi}{16-\pi^2}\frac{1}{\sqrt{\left(\alpha_m-\left(\alpha_n+\rho_{SE}^2\right)y\right)}}\sqrt{\frac{y}{\rho_E}}\right)}{\Gamma\left(\frac{\pi^2}{16-\pi^2}N\right)}\tag{B.2}$$

The PDFs of γ_{E_n} and γ_{E_m} are obtained by deriving (B.3) and (B.4) are displayed at the top of the page.

REFERENCES

[1] S. Arzykulov, G. Nauryzbayev, M. S. Hashmi, A. M. Eltawil, K. M. Rabie, and S. Seilov, "Hardware- and interference-limited cognitive IoT relaying NOMA networks with imperfect SIC over generalized non-homogeneous fading channels," *IEEE Access*, vol. 8, pp. 72942–72956, Apr. 2020.

[2] S. Buzzi, C.-L. I, T. E. Klein, H. V. Poor, C. Yang, and A. Zappone, "A survey of energy-efficient techniques for 5G networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 697–709, Apr. 2016.

[3] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[4] J. Zhao, "A survey of reconfigurable intelligent surfaces: Towards 6G wireless communication networks with massive MIMO 2.0," 2019, *arXiv:1907.04789*. [Online]. Available: https://arxiv.org/abs/1907.04789

[5] X. Mu, Y. Liu, L. Guo, J. Lin, and N. Al-Dhahir, "Exploiting intelligent reflecting surfaces in multi-antenna aided NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6884–6898, Oct. 2020.

[6] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, Aug. 2019.

[7] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.

[8] A. C. Tasolamprou *et al.*, "Exploration of intercell wireless millimeter-wave communication in the landscape of intelligent metasurfaces," *IEEE Access*, vol. 7, pp. 122931–122948, Aug. 2019.

[9] C. Huang, A. Zappone, M. Debbah, and C. Yuen, "Achievable rate maximization by passive intelligent mirrors," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2018, pp. 3714–3718.

[10] L. Subrt and P. Pechac, "Intelligent walls as autonomous parts of smart indoor environments," *IET Commun.*, vol. 6, no. 8, pp. 1004–1010, May 2012.

[11] M. M. Alani, "IoT lotto: Utilizing IoT devices in brute-force attacks," in *Proc. 6th Int. Conf. Inf. Technol., IoT Smart City (ICIT)*, 2018, pp. 140–144.

[12] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, "Beamforming design for physical layer security in a two-way cognitive radio IoT network with SWIPT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10786–10798, Dec. 2019.

[13] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[15] D. Xu and H. Zhu, "Secure transmission for SWIPT IoT systems with full-duplex IoT devices," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10915–10933, Dec. 2019.

[16] Z. Xiang, W. Yang, Y. Cai, Y. Cheng, H. Wu, and M. Wang, "Secrecy performance analysis of uplink NOMA in IoT networks," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Beijing, China, Aug. 2018, pp. 506–510.

[17] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure and reliable IoT communications using nonorthogonal Signals' superposition with dual-transmission," in *Proc. IEEE 31st Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, London, U.K., Aug. 2020, pp. 1–6.

[18] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[19] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–6.

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

[21] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, Jun. 2019.

[22] 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.

[23] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[24] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[25] G. Yang, X. Xu, and Y.-C. Liang, "Intelligent reflecting surface assisted non-orthogonal multiple access," 2019, *arXiv:1907.03133*. [Online]. Available: http://arxiv.org/abs/1907.03133

[26] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on IRS-NOMA," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1596–1600, Oct. 2020.

[27] C. Studer, M. Wenk, and A. Burg, "MIMO transmission with residual transmit-RF impairments," in *Proc. Int. ITG Workshop Smart Antennas (WSA)*, Feb. 2010, pp. 189–196.

[28] P. Zetterberg, "Experimental investigation of TDD reciprocity-based zero-forcing transmit precoding," *EURASIP J. Adv. Signal Process.*, vol. 2011, no. 1, pp. 1–10, Dec. 2011.

[29] X. Li, M. Huang, C. Zhang, D. Deng, K. M. Rabie, Y. Ding, and J. Du, "Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments," *IEEE Access*, vol. 7, pp. 102644–102661, Jul. 2019.

[30] X. Li, M. Liu, C. Deng, D. Zhang, X.-C. Gao, K. M. Rabie, and R. Kharel, "Joint effects of residual hardware impairments and channel estimation errors on SWIPT assisted cooperative NOMA networks," *IEEE Access*, vol. 7, pp. 135499–135513, Sep. 2019.

[31] X. Tian, Q. Li, X. Li, H. Zhang, K. Rabie, and C. C. Cavalcante, "Performance analysis of two-way relay noma systems with hardware impairments and channel estimation errors," *KSII Trans. Internet Inf. Syst.*, vol. 3, no. 6, pp. 134–156, May 2019.

[32] S. Zhou, W. Xu, K. Wang, M. Di Renzo, and M.-S. Alouini, "Spectral and energy efficiency of IRS-assisted MISO communication with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 9, no. 9, pp. 1366–1369, Sep. 2020.

[33] Y. Liu, E. Liu, and R. Wang, "Energy efficiency analysis of intelligent reflecting surface system with hardware impairments," 2020, *arXiv:2004.09804*. [Online]. Available: http://arxiv.org/abs/2004.09804

[34] F. Ding, H. Wang, S. Zhang, and M. Dai, "Impact of residual hardware impairments on non-orthogonal multiple access based amplify-and-forward relaying networks," *IEEE Access*, vol. 6, pp. 15117–15131, Mar. 2018.

[35] M. Li, B. Selim, S. Muhaidat, P. C. Sofotasios, M. Dianati, P. D. Yoo, J. Liang, and A. Wang, "Effects of residual hardware impairments on secure NOMA-based cooperative systems," *IEEE Access*, vol. 8, pp. 2524–2536, 2020.

[36] M. Baker, "From LTE-advanced to the future," *IEEE Commun. Mag.*, vol. 50, no. 2, pp. 116–120, 2012.

[37] X. Tan, Z. Sun, J. M. Jornet, and D. Pados, "Increasing indoor spectrum sharing capacity using smart reflect-array," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[38] A.-A.-A. Boulogeorgos and A. Alexiou, "Performance analysis of reconfigurable intelligent surface-assisted wireless systems and comparison with relaying," *IEEE Access*, vol. 8, pp. 94463–94483, May 2020.

[39] Y. Xu, J. Xia, H. Wu, and L. Fan, "Q-learning based physical-layer secure game against multiagent attacks," *IEEE Access*, vol. 7, pp. 49212–49222, Apr. 2019.

[40] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[41] A. Neumaier, *Introduction to Numerical Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1987.

QIN CHEN is currently pursuing the master's degree with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. Her main research interest includes the physical layer secrecy performance of non-orthogonal multiple access systems.

MEILING LI received the M.S. and Ph.D. degrees in signal and information processing from the Beijing University of Posts and Telecommunications, Beijing, in 2007 and 2012, respectively. She is currently a Professor with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. She is also a Visiting Research Scholar with the University of Warwick, U.K. Her research interests include cognitive radio, cooperative communications, non-orthogonal multiple access, and physical layer security technology.

XIAOXIA YANG is currently pursuing the master's degree with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. Her main research interest includes the physical layer secrecy performance of wireless networks.

RYAN ALTURKI received the Ph.D. degree from the University of Technology, Sydney, Australia. He is currently an Assistant Professor with the Department of Information Sciences, College of Computers and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia. His research interests include e-health, mobile technologies, the Internet of Things, and cyber security.

MOHAMMAD DAHMAN ALSHEHRI received the Ph.D. degree in artificial intelligence of cybersecurity for Internet of Things (IoT) from the University of Technology Sydney, Australia. He is currently an Assistant Professor with the Computer Science Department, Taif University, Saudi Arabia, and also a Visiting Professor with the School of Computer Science, University of Technology Sydney (UTS), Australia. He developed six smart novel algorithms for the IoT to reinforcement cybersecurity with AI that can detect various behaviors of cyber-attacks and provide full secure and protection platform for the IoT from the most harmful cyber-attacks. Furthermore, he published several publications in high ranked international journals, top-tier conferences, and chapters of books. His current research interests include cybersecurity, artificial intelligence, the Internet of Things (IoT), and trust and reputation. He also received a number of international and national awards and prizes.

FAZLULLAH KHAN (Senior Member, IEEE) received the Ph.D. degree in computer science from Abdul Wali Khan University Mardan, Pakistan. He is currently an Assistant Professor of computer science with Abdul Wali Khan University Mardan. His research interests include security and privacy, the Internet of Things, machine learning, and artificial intelligence. Recently, he has been involved in latest developments in the field of the Internet of Vehicles security and privacy issues, software-defined networks, fog computing, and big data analytics. He has served more than ten conferences in leadership capacities, including the General Chair, the General Co-Chair, the Program Co-Chair, the Track Chair, and the Session Chair. His research has been published in IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technologies, IEEE Access, *Computer Networks* (Elsevier), *Future Generations Computer Systems* (Elsevier), *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *Mobile Networks and Applications* (Springer). He has served as the Guest Editor for IEEE Journal of Biomedical and Health Informatics (JBHI) journal, *Multimedia Technology and Applications* (Springer), *Mobile Networks and Applications* (Springer), *Inderscience Big data Analytics*, and *Neural Computing and Applications* journal.

• • •