Reconfigurable Intelligent Surfaces-Aided Physical Layer Security Enhancement in D2D Underlay Communications

Majid H. Khoshafa, *Graduate Student Member, IEEE*, Telex M. N. Ngatched, *Senior Member, IEEE*, and Mohamed Hossam Ahmed, *Senior Member, IEEE*

***Abstract*—This letter investigates a reconfigurable intelligent surfaces (RIS)-aided wireless communication system in an inband underlay Device-to-Device (D2D) communication, where the direct link between D2D users is unavailable. An RIS is used to adjust its reflecting elements to enhance the D2D communication data transmission while improving the cellular network's secrecy performance concurrently. Specifically, analytical results for the secrecy outage probability and the probability of non-zero secrecy capacity are derived for the cellular network. Moreover, the D2D outage probability is also provided. Simulation and analytical results are presented to verify the derived expressions' correctness and the effectiveness of the proposed scenario. Moreover, the asymptotic results are presented.**

***Index Terms*—Reconfigurable intelligent surfaces, D2D communication, physical layer security.**

I. Introduction

RECONFIGURABLE Intelligent Surfaces (RIS), which is a surface of electromagnetic (EM) material that consists of a large number of inexpensive passive reflecting elements controlled by a microcontroller, have received significant consideration as a leading technologies in the sixth-generation (6G) wireless networks [1], [2]. There are many advantages of RIS such as the ability to control the transmission environment by directing the reflected signals in a specific direction and very low power consumption compared with relaying technology [3]. RIS have also been referred to as software-controlled metasurfaces [4] and intelligent reflecting surfaces [5]. On the other development, originally investigated by Wyner [6], physical layer security (PLS) has been developed as an appealing technique for enhancing cellular network security against eavesdropping attacks. Towards this end, PLS uses the natural properties and characteristics of wireless communication channels and noise to secure the data transmission by limiting the amount of data that can be leaked at the bit level by eavesdroppers. Thanks to their unique properties, which allows them the ability to control the transmission environment, RIS can be used for interference suppression and signal enhancement without the use of active transmitters. In this respect, RIS technology was recently investigated to improve the PLS of wireless communication system [7]–[9]. For channel estimation in RIS technology, efficient strategies were proposed in [10], [11].

Device-to-device (D2D) communication is of great interest as a pioneering technology in future cellular communications to overcome the spectrum scarcity problem. In scenarios where direct links are unfavorable for the D2D nodes, the relay-aided transmission plays an essential role in enhancing D2D communication's performance. For the relay-aided underlay D2D communication, the PLS was recently studied in [12], [13]. It was shown that multi-antenna relays can be used to enhance the reliability of the D2D transmission and the PLS of the cellular network concurrently. However, as lately demonstrated in [14], improving the data rate and reducing the implementation complexity can be achieved by utilizing RIS, which outperform the relay-aided communications. To the best of our knowledge, no work has been reported in the literature investigating the use of RIS to enhance the PLS of the cellular network and improve the D2D transmission link concurrently. The main contributions of this letter are listed as follows:

- The RIS is used to enhance the robustness and reliability of D2D communication, while simultaneously improving the PLS of the cellular network by generating jamming signals towards the eavesdropper.
- As compensation for spectrum sharing, the RIS serves as a friendly jammer to ensure a high-security level for the cellular network, thus enabling a win-win situation between the two networks, i.e., security provisioning for the cellular user and high reliability and robustness for the D2D users.
- The outage probability of D2D communication is investigated, and an analytical expression is obtained. Moreover, the cellular network's secrecy performance is analyzed, and closed-form expressions of the secrecy outage probability SOP) and the probability of non-zero secrecy capacity (PNSC) are also derived.
- Asymptotic analysis is provided to get more insights into the impact of the significant parameters of the proposed system on the performance of the SOP.
- The accuracy of our analyses is verified through intensive Monte-Carlo simulations.

Manuscript received October 27, 2020; revised November 22, 2020 and December 14, 2020; accepted December 14, 2020. Date of publication December 23, 2020; date of current version May 6, 2021. This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada under its Discovery Grant (DG) program (RGPINs 2019-04626 and 2014-03638). The associate editor coordinating the review of this letter and approving it for publication was G. Chen. *(Corresponding author: Majid H. Khoshafa.)*

Majid H. Khoshafa and Telex M. N. Ngatched are with the Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, NL A1B 3X5, Canada (e-mail: mhakhoshafa@mun.ca; tngatched@grenfell.mun.ca).

Mohamed Hossam Ahmed is with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada (e-mail: mahme3@uottawa.ca).

Digital Object Identifier 10.1109/LCOMM.2020.3046946

II. System Model

In this letter, we consider a D2D communication, including a single-antenna D2D transmitter, T, and a single-antenna D2D receiver, D, in Fig. 2. The D2D communication is underlying a cellular network consisting of a base station (BS), equipped with N_B antennas, communicating with a single-antenna cellular user, C, in the presence of a single-antenna eavesdropper, E. The direct path between T and D is not available due to severe shadowing caused by obstacles. Thus, the direct communication links between D2D users suffer high signal attenuation [15], [16]. An RIS is deployed on a surrounding building's facade to assist the D2D transmitter in overcoming the disadvantageous propagation conditions by giving high-quality virtual link from T to D, while serving as a jammer to E, resulting in an enhanced secrecy rate for the cellular user. The RIS is made of N reflecting elements. All communication channels are assumed to be independent, identical, slowly varying, flat, and their envelope follows Rayleigh distributions with a scale parameter equal to 1. Furthermore, we assume that the channel state information (CSI) of all channels, including E's channel, is perfectly available at the RIS for transmitting/reflecting data and jamming signals [7], [17], [18].

The channel coefficients for the T → RIS, RIS → D, RIS → E, BS → C, BS → D, and BS → E links are denoted as $\mathbf{h}_t$, $\mathbf{h}_d$, $\mathbf{h}_e$, h_{bc}, h_{bd}, and h_{be}, respectively. In addition, the Euclidean distances between T → RIS, RIS → D, RIS → E, BS → C, BS → D, and BS → E links are denoted as d_{tr}, d_{rd}, d_{re}, d_{bc}, d_{bd}, and d_{be}, respectively. The signals reflected by the RIS two or more times are neglected due to severe path loss. Thus, the received signal at D can be expressed as $y_D = \sqrt{P_d}\left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\frac{\eta}{2}}\left[\sum_{i=1}^{N} h_{t_i}\, g_i\, h_{d_i}\, x_d\right] + \sqrt{P_b}\left(\frac{d_{bd}}{d_o}\right)^{-\frac{\eta}{2}} h_{bd}\, x_b + n_d$, where d_o is a reference distance, P_d is the D2D transmission power, P_b is the BS transmission power, x_d and x_b are the D2D and BS transmitted signals, respectively, and n_d is the AWGN at D. g_i denotes the i^{th} reflecting meta-surfaces response of the RIS, and η denotes the path loss exponent. In addition, h_{t_i}, g_i, and h_{d_i} are complex Gaussian random variables (RV) with a zero mean and unit variance, where $g_i = |g_i| \exp(j\theta_i)$. Moreover, the phases of the channels h_{t_i}, and h_{d_i} are assumed to be completely available at the RIS.[1] Hence, the RIS element select the optimal phase shift as [1] $\theta_i = -(\phi_i + \varphi_i)$, where ϕ_i and φ_i are respectively the phases of h_{t_i} and h_{d_i}. Furthermore, we assume that the reflected gain of the i^{th} metasurface is equal to 1. The received signal at C can be expressed as $y_C = \sqrt{P_b}\left(\frac{d_{bc}}{d_o}\right)^{-\frac{\eta}{2}} h_{bc}\, x_b + n_c$, where n_c is the AWGN at C. In this respect, we assume that the received signals at C is not affected by the interference from T since it is located far away from C, and transmits with low power. Now, the received signal at E is given by $y_E = \sqrt{P_b}\left(\frac{d_{be}}{d_o}\right)^{-\frac{\eta}{2}} h_{be}\, x_b + \sqrt{P_d}\left(\frac{d_{tr}\, d_{re}}{d_o^2}\right)^{-\frac{\eta}{2}}\left[\sum_{i=1}^{N} h_{t_i}\, g_i\, h_{e_i}\, x_d\right] + n_e$, where h_{e_i} is the channel coefficient between the i^{th} element of the RIS and E, and n_e is the AWGN at E.

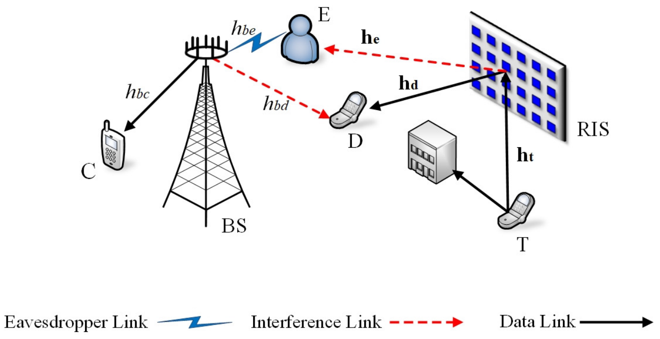

Fig. 1. The system model.

III. Performance Analysis

A. D2D Outage Probability

For the D2D communication, the outage probability, P_{out}, is defined by

$$P_{out} = \Pr\left(\gamma_D \leq \varphi\right) = F_{\gamma_D}(\varphi), \tag{1}$$

where $\varphi = 2^{\mathcal{R}_d} - 1$, $\mathcal{R}_d$ is the data rate of D2D transmission, and γ_D is the instantaneous end-to-end signal-to-interference-and-noise ratio (SINR) for the D2D link, γ_D, which is given by

$$\gamma_D = \frac{P_d\left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta}\left(\sum_{i=1}^{N}|h_{t_i}|\,|h_{d_i}|\right)^2}{\sigma_d^2 + P_b\left(\frac{d_{bd}}{d_o}\right)^{-\eta}|h_{bd}|^2} = \frac{\gamma_{td}}{1+\gamma_{bd}}, \tag{2}$$

where $\gamma_{td} = \bar{\gamma}_{td}\left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta}\left(\sum_{i=1}^{N}|h_{t_i}|\,|h_{d_i}|\right)^2$, $\gamma_{bd} = \bar{\gamma}_{bd}\left(\frac{d_{bd}}{d_o}\right)^{-\eta}|h_{bd}|^2$, $\bar{\gamma}_{td} = \frac{P_d}{\sigma_d^2}$, and $\bar{\gamma}_{bd} = \frac{P_b}{\sigma_d^2}$. Let us define $\omega_1 = \bar{\gamma}_{td}\left(\frac{d_{tr}\, d_{rd}}{d_o^2}\right)^{-\eta}$ and $\omega_2 = \bar{\gamma}_{bd}\left(\frac{d_{bd}}{d_o}\right)^{-\eta}$. The cumulative distribution function (CDF) of γ_D can be obtained using [19]

$$F_{\gamma_D}(\gamma) = \int_0^{\infty} F_{\gamma_{td}}(\gamma\,(\zeta+1))\, f_{\gamma_{bd}}(\zeta)\, d\zeta, \tag{3}$$

where $F_{\gamma_{td}}(.)$ is given by [14]

$$F_{\gamma_{td}}(\gamma) = \frac{\Upsilon\left(\xi+1, \mu\sqrt{\frac{\gamma}{\omega_1}}\right)}{\Gamma\left(\xi+1\right)}, \tag{4}$$

where $\xi = \frac{N\pi^2}{(16-\pi^2)} - 1$, $\mu = \frac{2\pi}{(16-\pi^2)}$, $\Gamma(.)$ is the gamma function [20, eq. (8.310.1)], and $\Upsilon\left(a, x\right) = \int_0^x t^{a-1}\exp\left(-t\right) dt$ is the lower incomplete gamma function defined by [20, eq. (8.350.1)]. On the other hand, $f_{\gamma_{bd}}(.)$ is given by $f_{\gamma_{bd}}(\gamma) = \frac{1}{\omega_2}\exp\left(-\frac{\gamma}{\omega_2}\right)$. By plugging (4) and $f_{\gamma_{bd}}(.)$ into (3), using series expansion in [20, eq. (8.354.1)], then with the help of

[1] Since this is an ideal situation, the results obtained represent an upper bound on the performance gain that can be achieved by the RIS.

[20, eq. (3.382.4)], $F_{\gamma_D}(\gamma)$ can be obtained as

$$F_{\gamma_D}(\gamma) = \frac{1}{\Gamma(\xi+1)\,\omega_2} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\mu \sqrt{\frac{\gamma}{\omega_1}}\right)^{\xi+n+1} \exp\left(\frac{1}{\omega_2}\right)}{n!\,(\xi+n+1)\;\omega_2^{-\left(\frac{\xi+n+3}{2}\right)}} \times \Gamma\left(\frac{\xi+n+3}{2}, \frac{1}{\omega_2}\right), \quad (5)$$

where $\Gamma(.,.)$ is the upper incomplete gamma [20, eq. (8.350.2)]. By plugging (5) into (1), P_{out} can be obtained.

B. Secrecy Outage Probability

The SOP can be expressed as [21]

$$\text{SOP} = \Pr\left(C_S < \mathcal{R}_s\right), \quad (6)$$

where C_S is the secrecy capacity, that is given by [22]

$$C_S = \begin{cases} C_C - C_E, & \gamma_C > \gamma_E, \\ 0, & \gamma_C \leq \gamma_E, \end{cases} \quad (7)$$

where C_C and C_E denote the cellular and eavesdropper capacities, respectively, and γ_C and γ_E are the SINR at C and E, respectively. In this regard, C_C is given by

$$C_C = \log_2\left(1+\gamma_C\right), \quad (8)$$

where γ_C is given by

$$\gamma_C = \frac{P_b \left(\frac{d_{bc}}{d_o}\right)^{-\eta} |h_{bc}|^2}{\sigma_c^2} = \gamma_{bc}, \quad (9)$$

where $\gamma_{bc} = \bar{\gamma}_{bc} \left(\frac{d_{bc}}{d_o}\right)^{-\eta} |h_{bc}|^2$ and $\bar{\gamma}_{bc} = \frac{P_b}{\sigma_c^2}$. Let us define $\omega_3 = \bar{\gamma}_{bc} \left(\frac{d_{bc}}{d_o}\right)^{-\eta}$. In addition, C_E can be obtained by

$$C_E = \log_2\left(1+\gamma_E\right), \quad (10)$$

where γ_E is given by

$$\gamma_E = \frac{P_b \left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2}{\sigma_e^2 + P_d \left(\frac{d_{tr}\,d_{re}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\,|h_{e_i}|\right)^2} = \frac{\gamma_{be}}{1+\gamma_e}, \quad (11)$$

where $\gamma_e = \bar{\gamma}_e \left(\frac{d_{tr}\,d_{re}}{d_o^2}\right)^{-\eta} \left(\sum_{i=1}^{N} |h_{t_i}|\,|h_{e_i}|\right)^2$, $\gamma_{be} = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta} |h_{be}|^2$, $\bar{\gamma}_{be} = \frac{P_b}{\sigma_e^2}$, and $\bar{\gamma}_e = \frac{P_d}{\sigma_e^2}$. Let us define $\omega_4 = \bar{\gamma}_{be} \left(\frac{d_{be}}{d_o}\right)^{-\eta}$, and $\omega_5 = \bar{\gamma}_e \left(\frac{d_{tr}\,d_{re}}{d_o^2}\right)^{-\eta}$.

To maximize the cellular capacity, the best transmit antenna at the BS is chosen based on the following criterion

$$k^* = \arg \max_{k=1,\ldots,N_B} C_{C_k} = \arg \max_{k=1,\ldots,N_B} \gamma_{C_k}. \quad (12)$$

The SOP is formulated as

$$\text{SOP} = \int_0^\infty F_{\gamma_C}\left(\beta\gamma+\alpha\right) f_{\gamma_E}(\gamma)\, d\gamma, \quad (13)$$

where $\beta = 2^{\mathcal{R}_s}$, $\alpha = \beta - 1$, and $F_{\gamma_C}(.)$ is given by

$$F_{\gamma_C}(\gamma) = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left(1 - \exp\left(-\frac{\gamma\,(k+1)}{\omega_3}\right)\right). \quad (14)$$

The PDF of γ_E can be derived using

$$f_{\gamma_E}(\gamma) = \int_0^\infty (x+1)\, f_{\gamma_{be}}\left(\gamma\,(x+1)\right) f_{\gamma_e}(x)\, dx, \quad (15)$$

where $f_{\gamma_{be}}(.)$ is given by

$$f_{\gamma_{be}}(\gamma) = \frac{1}{\omega_4} \exp\left(-\frac{\gamma}{\omega_4}\right), \quad (16)$$

and $f_{\gamma_e}(.)$ is given by [14]

$$f_{\gamma_e}(\gamma) = \frac{\mu^{\xi+1}}{2\,\Gamma(\xi+1)\,\omega_5^{\frac{\xi+1}{2}}}\, \gamma^{\frac{\xi-1}{2}} \exp\left(-\mu\sqrt{\frac{\gamma}{\omega_5}}\right). \quad (17)$$

By substituting (16) and (17) in (15), and utilizing [23, eq. (07.34.03.0606.01)] and [24, eq. (07.34.03.0228.01)], then [20, eq. (7.811.1)], $f_{\gamma_E}(\gamma)$ can be obtained as

$$f_{\gamma_E}(\gamma) = \frac{\Delta}{\exp\left(\frac{\gamma}{\omega_4}\right)} \left[\frac{1}{\gamma}\, G_{2,1}^{1,2}\left(\frac{\gamma}{\omega_4\,\mathcal{Q}_1^2} \,\middle|\, \begin{matrix} \frac{-\xi+1}{2}, \frac{-\xi}{2} \\ 1 \end{matrix}\right) + \frac{1}{\omega_4} G_{2,1}^{1,2}\left(\frac{\gamma}{\omega_4\,\mathcal{Q}_1^2} \,\middle|\, \begin{matrix} \frac{-\xi+1}{2}, \frac{-\xi}{2} \\ 0 \end{matrix}\right)\right], \quad (18)$$

where $\Delta = \frac{\mu^{\xi+1}\,\mathcal{Q}_1^{-(\xi+1)}}{2\sqrt{\pi}\,\Gamma(\xi+1)\,\omega_5^{\left(\frac{\xi+1}{2}\right)}}$, $\mathcal{Q}_1 = \left(\frac{\mu}{2\sqrt{\omega_5}}\right)$, and $G_{p,q}^{m,n}\left(x \,\middle|\, \begin{matrix} a_p \\ b_q \end{matrix}\right)$ represents the Meijer *G*-function [20, (9.301)]. Now, the SOP can be derived as in (19) at the bottom of the page by plugging (14) and (18) into (13), and utilizing [24, eq. (07.34.03.0228.01)], then [20, eq. (7.811.1)], where $\mathcal{Q}_2 = \left(\frac{1}{\omega_4} + \frac{(k+1)\beta}{\omega_3}\right)$.

$$\text{SOP} = N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \left[1 - \left(\frac{\Delta}{\mathcal{Q}_1^{-2}} \exp\left(-\frac{(k+1)\,\alpha}{\omega_3}\right) \left[\mathcal{Q}_2\,\omega_4\, G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\,\mathcal{Q}_2\,\omega_4 \,\middle|\, \begin{matrix} -1 \\ -1, \frac{\xi-1}{2}, \frac{\xi}{2} \end{matrix}\right) + G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\,\mathcal{Q}_2\,\omega_4 \,\middle|\, \begin{matrix} 0 \\ 0, \frac{\xi-1}{2}, \frac{\xi}{2} \end{matrix}\right)\right]\right)\right] \quad (19)$$

C. Asymptotic Secrecy Outage Analysis

To acquire more insights on the system design, the asymptotic SOP, SOP$^\infty$, is examined. SOP$^\infty$ can be written as

$$\mathrm{SOP}^\infty \approx (\mathcal{G}_a \omega_3)^{-\mathcal{G}_d}, \tag{20}$$

where $\mathcal{G}_d$ and $\mathcal{G}_a$ are the secrecy diversity order and the secrecy array gain, respectively. Mathematically speaking, to derive the SOP$^\infty$, the asymptotic CDF, $F_{\gamma_C}^{\infty}(.)$, is derived and then plugging into (13), and using [20, eq. (7.813.1)]. After performing some algebraic manipulations, it turns out that $\mathcal{G}_d = N_B$ and $\mathcal{G}_a$ is given by

$$\mathcal{G}_a = \Bigg[\Delta\,\alpha^{N_B} \sum_{k=0}^{N_B} \binom{N_B}{k} \left(\frac{\omega_4\,\beta}{\alpha}\right)^{k} G_{3,1}^{1,3}\left(\frac{1}{\mathcal{Q}_1^2} \,\middle|\, \begin{matrix} 1-k\,, \frac{-\xi+1}{2}\,, \frac{-\xi}{2} \\ 1 \end{matrix}\right)\Bigg]^{\frac{-1}{N_B}}.$$

D. Probability of Non-Zero Secrecy Capacity

The non-zero secrecy capacity is obtained when $\gamma_C > \gamma_E$. From (7), the PNSC is given by

$$\mathrm{PNSC} = \Pr\left(\frac{1+\gamma_C}{1+\gamma_E} > 1\right) = 1 - \int_0^\infty F_{\gamma_C}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma. \tag{21}$$

By plugging (14) and (18) into (21), and following the same procedure as in the derivation of (19), the PNSC can be derived as in (22) at the bottom of the page, where $\mathcal{Q}_3 = \left(\frac{1}{\omega_4} + \frac{(k+1)}{\omega_3}\right)$.

IV. Results and Discussions

In this section, we present the numerical results of the D2D outage probability, the SOP of the cellular network, and the PNSC to validate the analytical analysis. In this respect, the cellular network's secrecy performance is analyzed, and the influence of the RIS is examined. The main parameters utilized to obtain the numerical and simulation results are set as $\omega_4 = 20$ dB, $\omega_5 = 0$ dB, $N_B = 4$, $\mathcal{R}_b = 1$ b/s/Hz, $\mathcal{R}_s = 1$ b/s/Hz, and $\sigma_\upsilon^2 = 1$, where $\upsilon \in \{d, c, e\}$.

Figure 2 plots the analytical and simulation results of the outage probability of the RIS-assisted D2D P_{out}, versus ω_1, for different values of N at the RIS. For comparison purposes, the outage probability of single AF-relaying D2D communication is presented. As shown P_{out} of the D2D link decreases dramatically when ω_1 increases. Interestingly, as the number of elements N increases, P_{out} improves significantly. Consequently, the reliability of D2D communication increases. As a result, it can be infer that for a given D2D outage probability requirement, the RIS's energy efficiency can be enhanced by increasing N. To illustrate, ω_1 can be decreased by approximately 15 dB, using an RIS with $N = 10$ compared with $N = 4$ to achieve the D2D outage probability of 10^{-4}. It is worth mentioning that RIS-assisted system outperforms the AF-relaying system. To show the performance loss caused by discrete phase shifts, we provide simulation results with the phase error of each reflector uniformly distributed in $\left\{-\frac{\pi}{2^2}, \frac{\pi}{2^2}\right\}$ [25]. Furthermore, the simulation and numerical results agree perfectly, confirming the accuracy of our results.

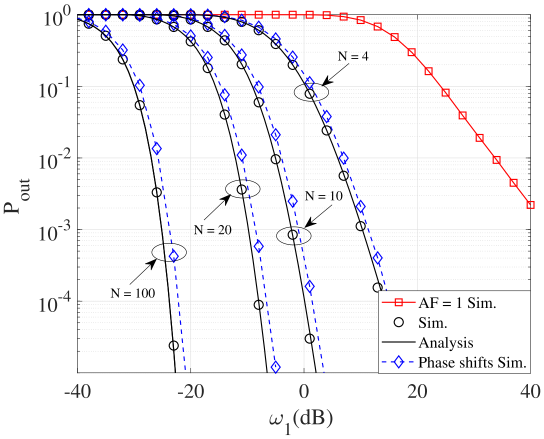

Fig. 2. The D2D outage probability, where $\mathcal{R}_b = 1$ b/s/Hz.

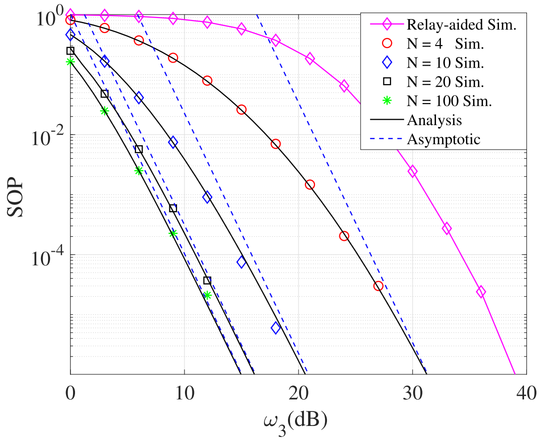

Fig. 3. The SOP of cellular network, where $\omega_4 = 20$ dB, $\omega_5 = 0$ dB, $N_B = 4$, and $\mathcal{R}_s = 1$ b/s/Hz.

The SOP is shown in Fig. 3 versus ω_3 for different values of N. Notably, the SOP decreases as N increases, demonstrating the influence of the jamming signals from RIS on E. Therefore, the security of the data transmission is enhanced. Moreover, the SOP decreases as ω_3 increases. To illustrate, ω_3 can be decreased by approximately 10 dB, using an RIS with $N = 10$ compared with $N = 4$ to achieve an SOP of 10^{-4}. As a benchmark, the SOP of the AF-relaying

$$\mathrm{PNSC} = 1 - N_B \sum_{k=0}^{N_B-1} \frac{(-1)^k \binom{N_B-1}{k}}{(k+1)} \Bigg[1 - \Bigg(\frac{\Delta}{\mathcal{Q}_1^{-2}} \Bigg[\mathcal{Q}_3\,\omega_4\, G_{1,3}^{3,1}\left(\mathcal{Q}_1^2 \mathcal{Q}_3 \omega_4 \,\middle|\, \begin{matrix} -1 \\ -1, \frac{\xi-1}{2}, \frac{\xi}{2} \end{matrix}\right) + G_{1,3}^{3,1}\left(\mathcal{Q}_1^2\, \mathcal{Q}_3\, \omega_4 \,\middle|\, \begin{matrix} 0 \\ 0, \frac{\xi-1}{2}, \frac{\xi}{2} \end{matrix}\right)\Bigg]\Bigg]\Bigg)\Bigg] \tag{22}$$

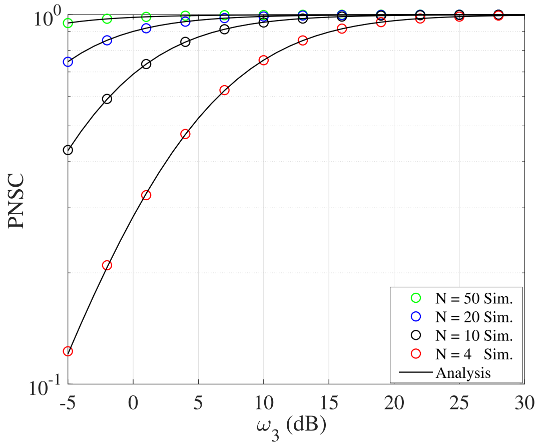

Fig. 4. The PNSC of cellular network, where $\omega_4 = 20$ dB, $\omega_5 = 0$ dB, and $\mathcal{R}_s = 1$ b/s/Hz.

D2D communication [26] is provided. As revealed in our analysis and simulation, improved secrecy performance can be achieved using RIS compared to the relay-aided scenario. This is due to the fact that the eavesdropping signal is degraded at E due to the jamming signals produced by RIS, which in turn results in more secure cellular transmission. To illustrate, ω_3 can be decreased by approximately 15 dB, using an RIS with $N = 10$ compared with relay-aided scenario to achieve an SOP of 10^{-4}. With this in mind, the asymptotic results are also presented, and an excellent match with the exact ones can be observed as $\omega_3 \rightarrow \infty$. This also confirm the accuracy of the expressions of $\mathcal{G}_a$ and $\mathcal{G}_d$.

Figure 4 illustrates the cellular PNSC versus ω_3, where the analytical result is provided by (22). Interestingly, the PNSC improves as N increases, showing the benefits of using RIS. Additionally, as ω_3 increases, the PNSC increases, implying an improvement in the security level of the cellular network. It is worth mentioning that the non-zero secrecy capacity exists even when the eavesdropper's channel has a higher average SNR as compared to main channel i.e., $\gamma_E > \gamma_C$. Simulation results are shown to conform with the analytical results, validating the analysis.

V. Conclusion

In this letter, RIS technology is investigated to enhance the reliability and robustness of D2D communication and improve the security level of the cellular network concurrently. New analytical expressions are derived for the cellular SOP and PNSC, and the D2D outage probability. The accuracy of these expressions are verified through Monte-Carlo simulations.

References

[1] 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, Jul. 2019.

[2] C. Huang *et al.*, “Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends,” *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[3] Q. Wu and R. Zhang, “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,” *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[4] 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.

[5] C. Huang, R. Mo, and C. Yuen, “Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, Aug. 2020.

[6] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] X. Guan, Q. Wu, and R. Zhang, “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?” *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[8] Z. Chu, W. Hao, P. Xiao, and J. Shi, “Intelligent reflecting surface aided multi-antenna secure transmission,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[9] 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.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[10] B. Zheng, C. You, and R. Zhang, “Intelligent reflecting surface assisted multi-user OFDMA: Channel estimation and training design,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 8315–8329, Dec. 2020.

[11] B. Zheng and R. Zhang, “Intelligent reflecting surface-enhanced OFDM: Channel estimation and reflection optimization,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 518–522, Apr. 2020.

[12] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided Device-to-Device communications,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

[13] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, “Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.

[14] 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, Jun. 2020.

[15] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, “Reconfigurable intelligent surfaces for energy efficiency in wireless communication,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[16] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, “Robust and secure wireless communications via intelligent reflecting surfaces,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[17] 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.

[18] 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.

[19] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

[20] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.

[21] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[22] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[23] Wolfram Research. (Oct. 2001). *The Wolfram Functions Site*. [Online]. Available: http://functions.wolfram.com/07.34.03.0606.01

[24] Wolfram Research. (Oct. 2001). *The Wolfram Functions Site*. [Online]. Available: http://functions.wolfram.com/07.34.03.0228.01

[25] P. Xu, G. Chen, G. Pan, and M. Di Renzo, “Ergodic secrecy capacity of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers,” *IEEE Wireless Commun. Lett.*, early access, 2020, doi: 10.1109/LWC.2020.3044178.

[26] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” *IEEE Access*, vol. 8, pp. 53575–53586, Mar. 2020.