Future Generation Computer Systems 126 (2022) 330–339

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Physical layer security for Internet of Things via reconfigurable intelligent surface

Dinh-Thuan Do [a,*], Anh-Tu Le [b], Nhat-Duy Xuan Ha [b], Nhu-Ngoc Dao [c]

[a] Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712, USA
[b] Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City, Viet Nam
[c] Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea

ARTICLE INFO

Article history:
Received 26 January 2021
Received in revised form 20 July 2021
Accepted 17 August 2021
Available online 25 August 2021

Keywords:
Internet of Things
Reconfigurable intelligent surface
Secrecy outage probability
Secrecy rate

ABSTRACT

Security countermeasures are considered one of the major concerns in the emerging Internet of Things (IoT) paradigm to guarantee an efficient network operation. To investigate the security problem in unauthorized access to sensitive IoT information and services, this paper, particularly, studies physical-layer security of a typical system model constituted by a reconfigurable intelligent surface (RIS) assisted access point (AP), legitimate user, and an eavesdropper. In this model, a RIS is deployed to increase the system secrecy and communication performances to deal with eavesdropping attacks. To measure the security performances, we firstly expose analytical results for the secrecy outage probability. We provide insights with asymptotic analysis to identify system parameters that significantly affect the secrecy performance of our proposed RIS-aided IoT systems. In particular, the findings show that by controlling the number of metasurface elements of the RIS and the average signal-to-noise ratios (SNR), system performances can be improved. We verify such a RIS-aided IoT system within many practical situations by conducting Monte-Carlo simulations in the Matlab simulation platform. We compared our analytical results with the Monte-Carlo simulations to evaluate the accuracy of the proposed closed-form expressions of secure performance metrics. Simulation results demonstrated that the secrecy performance in the IoT systems can be significantly improved by increasing the number of metasurfaces in the RIS and reducing channel quality approaching to eavesdroppers.

1. Introduction

To achieve ubiquitous connectivity, Internet of Things (IoT) systems have been deployed with a massive number of physical objects, such as sensors, controllers, and actuators. However, due to fundamental properties of broadcast and superposition in the wireless medium, wireless transmissions are inherently vulnerable to security concerns in emerging IoT systems [1–3]. Unlike conventional cryptographer encryption methods implemented in the application layer, physical layer security (PLS) relies on advanced signal processing approaches to guarantee secure wireless communications, which has attracted great attention in industry and academia [4]. By exploiting the intrinsic randomness of fading and the noise characteristics of wireless communication channels, PLS-based IoT systems are able to limit the impacts of potential eavesdroppers once they intend to extract amount of information from legitimate links. PLS techniques can enhance the secure performance of IoT networks since it can help IoT networks to reduce the latency of authentication, especially in mobile scenarios [5–9].

However, in traditional communication technologies, the propagation properties of wireless channels cannot be adaptively controlled to achieve desirable secure communication. To cope with these issues, reconfigurable intelligent surface (RIS)-aided transmission has been recommended to be promising techniques to achieve energy and spectral efficient communications. Constituted by low-cost reflecting elements, RIS can significantly improve the performance of wireless communication networks at capability of security within a reasonable cost [10,11]. RIS can be designed as a programmable passive reflecting array. To enhance propagation conditions, signals transmitted from the base station (BS) are reflected by the RIS to enhance mobile coverage and transmission quality. Since RIS consumes very low power and uses the limited spectrum resources more efficiently, RIS-aided systems offer better energy and spectrum efficiencies compared to conventional relaying systems.

Although the secrecy rate was analyzed in existing works [12–21] in the context of RIS, there still exists open problems to address PLS incorporation with RIS deployments in such an IoT system. In particular, we emphasize on current concerns in such

* Corresponding author.
E-mail addresses: dodinhthuan@utexas.edu (D.-T. Do), leanhtu@iuh.edu.vn (A.-T. Le), duyha.iuh@gmail.com (N.-D.X. Ha), nndao@sejong.ac.kr (N.-N. Dao).

https://doi.org/10.1016/j.future.2021.08.012
0167-739X/

a RIS-aided system relying on PLS in two folds: *(i) How RIS benefits to improve the quality of received signals at intended IoT devices?; (ii) Due to high cost and the system complexity in existing systems (as reported in [22–24]), by which the PLS technique can acquire the RIS to enhance secure performance metrics. For example, a simple closed-form expression of secure metric can be introduced to indicate secure performance degradation due to eavesdropper's signal and how many reflectors in a RIS should to be activated to obtain a predefined requirements in terms of secrecy outage probability and secrecy rate are of important issues. To the best of our knowledge, a few work have been performed to investigate the above problems yet. On the other hand, it is difficult to evaluate specific main factors based on exact formulas of secure outage probability. Hence, an approximation for such secure performance metrics should be derived in a closed-form expression while the transmit signal to noise ratio (SNR) is high. By doing so, the gaps between approximate and exact secure performances associated in both cases of single and multiple RIS elements should be quantified. We expect the simulation results indicate the small gaps between* of the approximated and exact formulas of secure outage probability, and exhibit the advances of the RIS-assisted system.

Briefly, the meaningful contributions of this paper can be summarized as follows:

- We propose a point-to-point RIS-aided IoT system by exploring secure performance of a source/destination pair [20,21], where deployment of the RIS is efficiently utilized to support the transmission between an AP and dedicated IoT device with respect to extended coverage.
- In the literature, research on the optimization problem of the phase-shifts design has not been still completely studied yet, hence, we consider the upper case of formula of SNR as a relevant approach to tackle the secure performance analysis in recent studies [12–21]. Moreover, we utilize closed-form expressions of secure performance metrics such as secure outage probability and secrecy capacity to further investigate suitable system parameters to achieve performance improvement of the RIS-aided IoT system.
- Due to lack of detailed research on configuration of RIS in term of the number of metasurface elements (denoted as N), we aim to consider different mathematical analysis on two representative cases of RIS configuration, i.e. $N = 1$ and $N \geqslant 2$ to show explicit computations in term of secure performance metrics as expected.

The remaining sections of this article are organized as follows. Related works are introduced in Section 2. Section 3 presents practical scenarios of secure RIS-aided IoT system along with signal processing at physical layer. In Section 4, we compute the closed-form expressions of secure performance metrics which rely on the expressions of SNR related to legitimate and eavesdropping devices. In Section 4, we also propose approximate computations for secure outage behavior. Then, we provide the numerical results along with detailed discussions in Section 5 before we conclude the study based on our main findings in Section 6.

2. Related work

2.1. Security in wireless IoT systems

In the literature, most of studies have been conducted to address technical issues of PLS deployments in wireless networks along with improved security performance. As potential benefit, PLS can assist 5G IoT networks reduce the latency of authentication, especially in presence of eavesdropping signals [26–28]. Once users roam in different BSs or APs, frequent authentication handovers are required. Such procedure may affect communication performance since it introduces large authentication overhead. By this way, PLS can offer an efficient and direct authentication by exploring the radio frequency (RF) fingerprint. As a result, the handshake process can be simplified and the authentication latency is reduced. Another benefit of PLS schemes is that an additional level of protection can cooperate with the existing security approaches and it provides highly effective safeguard for massive IoT devices. For example, the authors in [26] considered cooperative jammer beamforming under the context of a relay selection-based wireless system which selects suitable relays from the group of intermediate relays. On the other hand, the considered system treats the remaining nodes as friendly jammers. The authors determined jammer puts weights to null the destination's jamming signals at the destination and maximize the jamming signal at the eavesdropper [26]. A robust beamforming design was introduced for multiuser multiple antennas secrecy networks with simultaneous wireless information and power transfer in [27]. In such a system, an AP employs artificial noise (AN) generation to facilitate efficient wireless energy transfer and secure transmission with respect to serve multiple IoT devices. The work in [28] studied AN-aided secrecy beamforming for secure transmission, cooperative jamming (CJ) to further evaluate secure downlink transmission from a controller associated with an actuator. The controller needs the assistance of a cooperative jammer to fight against multiple passive and non-colluding eavesdroppers. To provide secrecy enhancing transmit design, the optimal secrecy outage probability (SOP) is derived subject to a minimum requirement on the secrecy rate [28].

2.2. Security in RIS-aided IoT systems

PLS takes benefits of the dynamic nature of wireless communication channels which can be intelligent controlled. As a result, PLS allows legitimate users can successfully decode the data while preventing eavesdroppers from decoding the data. More importantly, PLS does not require secret keys and complicated encryption processing in comparation with traditional cryptography. As far as we know, existing studies [16–21] focused on a part of secure performance metrics such as secrecy rate while research on secure outage probability and secrecy rate for RIS networks is still missing in the literature. For example, the authors in [13] explored secrecy rate in the RIS-based multi-antenna systems from the PLS perspective. They proposed an efficient alternating algorithm to maximize the system secrecy rate by considering the condition of the source transmit power and the unit modulus constraints imposed on phase shifts at the RIS. In [15], the authors studied maximization of the system sum-rate while limiting the maximum information leakage to the potential eavesdroppers by the joint designing the beamformers at the access point and the phase shifters at the RISs. The work in [16] proposed an effective algorithm to jointly optimize the active and passive beamforming by assuming a single-antenna legitimate user and a multi-antenna eavesdropper. In the proposed algorithm, the optimal transmit beamforming vector can be achieved at the BS under fixed RIS phase shifts. To exhibit the optimal secrecy rate, the phase elements at the RIS and the transmit beamforming vector at the BS can be jointly optimized as recently studied [17]. Shen et al. [19] investigated secure transmission optimization for RIS-aided multi-antenna systems by considering the optimal system secrecy rate subject to the unit modulus constraints the source and transmit power constraint imposed on phase shifts at the RIS. The authors in [21] studied a RIS-MIMO system, where a multi-antenna BS sends the data stream to multiantenna legitimate users which co-exist

Table 1
Comparison of proposed system with similar work.

Reference	Scenario	Comparison	System performance metrics
Our work	One AP, one legitimate user, and eavesdropper	RIS with $N = 1$, $N \geqslant 2$	Secure outage probability, average secrecy capacity and the approximation of secrecy outage probability
[15]	One BS, one legitimate user (Bob), one eavesdropper (Eve)	With and without RIS	Secrecy rates at Bob and Eve
[18]	Two legitimate users, and untrusted user	No	Sum-secrecy rate
[19]	One source, one RIS, one legitimate receiver, and one eavesdropper	No	Secrecy rate
[20]	One AP, K legitimate users, an eavesdropper and L RIS	No	Average system secrecy rate, average system energy efficiency
[25]	One BS, two legitimate users, an eavesdropper	RIS	Secure outage probability

with multiple antennas eavesdropper. In terms of optimizing the beamforming policy, they considered a suboptimal secrecy rate maximization approach. However, due to low-cost requirements, a unique framework is necessary to evaluate enough main secure performance metrics for possible application in IoT. We then provide a necessary comparison between our proposed system and similar works, shown in Table 1.

3. The practical scenarios of secure transmission employing RIS-assisted IoT systems

3.1. The practical scenarios

We consider a downlink of a particular group of devices that belong to the coverage of the access point serving multiple IoT devices under the perceptive of IoT system. In particular, an AP communicate to an IoT device via a RIS in the presence of an eavesdropper. In the principle of RIS with N metasurface elements, each reflective element is assumed to be able to be independently adjusted the phase of its reflected electromagnetic waves to boost the performance of the end-to-end communication. By programmable controlling over the phase-shift matrix at the RIS, it exhibits an intelligent way to serve IoT devices (legitimate and eavesdropping devices).[1] The half-duplex transmission mode is adopted to the AP, IoT device, and the eavesdropper. It is worth noting that the eavesdropper in this scenario can overhear signals transmitted from the RIS. In particular, we consider a practical system model where direct links between the AP and the legitimate device (or the eavesdropper) do not exist due to unwanted obstacles. Let P_S denotes the transmit power of the AP to the IoT device D on subcarrier m. The total transmit power of the access point is strictly limited by the maximum value P_{max}. The peak transmit power on each subcarrier is also restricted as $P_S < P_{peak}$. The scheduled transmission time is assumed to be normalized to be 1. For the availability of the channel power gains, we assume that the channel state information (CSI) on all the channel power gains is available at the AP and the IoT devices. Main denotations are summarized in Table 2.

We recommend possible applications in IoT systems as follows

- The IoT applications of 6G cellular networks, where the AP needs the assistance of RIS to directly talk to each IoT device to mitigate weak signal received at destinations due to obstacle or bad quality of transmission. From a PLS perspective, we treat the eavesdropper's signal affecting main devices as unwanted interference from surrounding IoT nodes.
- Since the actuators in industrial IoT (IIoT) need reliable transmission from a central controller or smart grid in the context of PLS systems, we deploy RIS to flexible improve signals' quality as needed.
- Since massive devices using bluetooth technique are treated as a low-energy wireless technique for short-range communications (possible kinds of devices such as healthcare devices, smartphones, and laptops), our study on RIS is a suitable way to improve serving coverage area for huge number of IoT devices. Therefore, together with guarantee transmission for bluetooth communications, secure and reliable transmissions are strictly required.

Regarding the role of the network layer of a conventional secure communication network, information security normally relies on cryptographer encryption which suffers from the vulnerabilities, such as secret key distribution, protection, and management. Different from techniques applied in the network layer security approach, the PLS can guarantee good security performance bypassing the relevant manipulations on the secret key. In wireless systems, an eavesdropper can attack at various layers including the physical layer. In the scope of this paper, we conduct the performance analysis for a pair of an AP and IoT

Table 2
The main denotations in the considered system.

Symbol	Description
N	The number of elements in RIS
x	The signal of access point (S)
P_S	The transmit power at S
$h_{R,n}$	The channel gain between S and RIS
$h_{D,n}$	The channel between RIS and destination (D)
$h_{E,n}$	The channel between RIS and eavesdropper (E)
δ_n	The reflection coefficient generated by the nth reflector of RIS
n_D and n_E	The additive white Gaussian noise (AWGN) with $\mathcal{CN}(0, N_0)$
β	The path-loss coefficient
d_R	The distance from S to RIS
d_D	The distance from RIS to D
d_E	The distance from RIS to E
θ_n and φ_n	The phases of the channel gains
$K_n(x)$	The modified Bessel function of the second kind
$I_\nu(x)$	The modified Bessel function of the first class with order ν
$Q_m(a; b)$	The Marcum Q-function
$\Gamma(\bullet)$	The complete gamma function
$\gamma(\bullet, \bullet)$	The lower incomplete gamma function
$\Gamma(\bullet, \bullet)$	The upper incomplete gamma function
$W_{p,q}(\bullet)$	The Whittaker function of the second kind
$G_{p,q}^{m,n}(\bullet)$	The Meijer's G-function

[1] We treat our system model as a point-point communication network that suffers from an external passive eavesdropper. We also reduce costs by designing a single antenna for all devices. Interestingly, to support the WiFi Protected Access (WPA) for the MAC layer encryption or for Transport Layer Security (TLS), the secret key can be achieved from this PLS procedure deployed in RIS-aided IoT systems. This is a further study and beyond the scope of this paper.

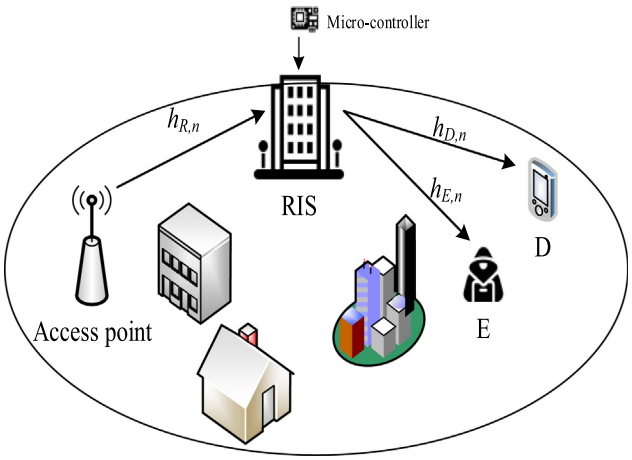

Fig. 1. System model.

device (legitimate) along with the existence of an eavesdropper, shown in Fig. 1, which is similar to the system model reported in [15,18,19].[2]

3.2. Signal processing at physical layer

To proceed received signal computation, we conduct information processing for distant devices. The received signal at D and E are given as respectively

$$y_D = \sqrt{P_S}\sum_{n=1}^{N} h_{R,n}h_{D,n}\delta_n x + n_D, \tag{1}$$

$$y_E = \sqrt{P_S}\sum_{n=1}^{N} h_{R,n}h_{E,n}\delta_n x + n_E \tag{2}$$

where $\delta_n = \varpi_n(\phi_n)e^{j\phi_n}$ denotes the reflecting coefficient generated by the nth reflector of the RIS, in which $\varpi_n(\phi_n)$ denotes the ideal phase shifts ($n = 1, \ldots, N$), $h_{R,n}$, $h_{D,n}$, $h_{E,n}$ are the channel gains with $h_{R,n} = \sqrt{d_R}^{-\beta} g_{R,n}e^{-j\theta_n}$, $h_{D,n} = \sqrt{d_D}^{-\beta} g_{D,n}e^{-j\varphi_n}$ and $h_{E,n} = \sqrt{d_E}^{-\beta} g_{E,n}e^{-j\varphi_n}$, where d_R, d_D and d_E are the distances from S to RIS, RIS to D and RIS to E, respectively, β denotes the path-loss coefficient, $g_{R,n}$, $g_{D,n}$, $g_{E,n}$ are the amplitudes of channel and following independent distributed Rayleigh random variables (RVs), θ_n and φ_n are the phases of the channel gains. It is assumed the phases of channel gain have the full knowledge at receivers. By this way, we compute the SNR at D as

$$\gamma_D = \frac{P_S\left|\sum_{n=1}^{N} g_{R,n}g_{D,n}e^{j\phi_n - j\varphi_n - j\theta_n}\right|^2}{(d_R d_D)^{\beta} N_0}. \tag{3}$$

Then, we need to eliminate the phases of channel to (2) is maximum. As recent work in [30], we set $\phi_n = \theta_n + \varphi_n$. Then, the maximization of γ_D is given as

$$\gamma_D = \frac{P_S\left[\sum_{n=1}^{N} g_{R,n}g_{D,n}\right]^2}{(d_R d_D)^{\beta} N_0} = \bar{\gamma}_D X_1^2, \tag{4}$$

where $X_1 = \sum_{n=1}^{N} g_{R,n}g_{D,n}$, $\bar{\gamma}_D = \frac{P_S}{(d_R d_D)^{\beta} N_0}$ denotes the average SNR. Similarly, the SNR at E is given by

$$\gamma_E = \frac{P_S\left[\sum_{n=1}^{N} g_{R,n}g_{E,n}\right]^2}{(d_R d_E)^{\beta} N_0} = \bar{\gamma}_E X_2^2, \tag{5}$$

where $X_2 = \sum_{n=1}^{N} g_{R,n}g_{E,n}$ and $\bar{\gamma}_E = \frac{P_S}{(d_R d_E)^{\beta} N_0}$ is the average SNR. The maximum achievable secrecy capacity is defined by [31]

$$C_S = \max\left\{\log_2(1+\gamma_D) - \log_2(1+\gamma_E), 0\right\}. \tag{6}$$

4. Secrecy performance analysis

In this section, we analyze the secure system performance metrics, namely secure outage probability and secrecy rate. To provide more insights in the RIS-aided IoT system, an asymptotic analysis is presented as well.

4.1. Secure outage probability

The secure outage probability (SOP), which is defined as the probability that secure communication can be realized, is a typical performance measure for RIS system relying on PLS. In particular, the SOP of such IoT system is written as

$$SOP = \Pr(C_S < C_{th}) = \Pr\left(\frac{1+\gamma_D}{1+\gamma_E} < \gamma_C\right), \tag{7}$$

where $\gamma_C = 2^{C_{th}}$, C_{th} denotes the target secrecy rate. Then, we can rewrite (7) as

$$\begin{aligned} SOP &= \Pr(\gamma_D < \gamma_C + \gamma_C\gamma_E - 1) \\ &= \int_0^{\infty} F_{\gamma_D}(\gamma_C + \gamma_C s - 1) f_{\gamma_E}(s)\, ds. \end{aligned} \tag{8}$$

4.1.1. Case N = 1

In this case, the probability density function (PDF) of g is written as $f_g(x) = \frac{2x}{\sigma^2}e^{-\frac{x^2}{\sigma^2}}$ with parameter σ. Thus, we denotes $X = X_1 = X_2$ with $\sigma = 1$ and after some transform we can write the PDF of X as [32]

$$f_X(x) = 4xK_0(2x), \tag{9}$$

where $K_n(x)$ denotes the modified Bessel function of the second kind [33, Eq. 3.324.1]. Moreover, the PDF and cumulative distribution function (CDF) of γ_r with $r \in \{E, D\}$ can be obtained as

$$f_{\gamma_r}(x) = \frac{2}{\bar{\gamma}_r}K_0\left(2\sqrt{\frac{x}{\bar{\gamma}_r}}\right), \tag{10}$$

and

$$F_{\gamma_r}(x) = 1 - 2\sqrt{\frac{x}{\bar{\gamma}_r}}K_1\left(2\sqrt{\frac{x}{\bar{\gamma}_r}}\right). \tag{11}$$

In here, we put (10) and (11) into (8), the SOP is rewritten by

$$\begin{aligned} SOP = 1 - \frac{4}{\bar{\gamma}_E}\int_0^{\infty} &\sqrt{\frac{(\gamma_C + \gamma_C s - 1)}{\bar{\gamma}_D}} \\ &\times K_0\left(2\sqrt{\frac{s}{\bar{\gamma}_E}}\right) K_1\left(2\sqrt{\frac{(\gamma_C + \gamma_C s - 1)}{\bar{\gamma}_D}}\right) ds. \end{aligned} \tag{12}$$

[2] Although we are able to utilize many RISs to increase the signal coverage to improve the communication quality of legitimate devices, the near eavesdropper directly communicates with the dedicated RIS [29]. There are multiple levels of interference among these RISs and hence degraded secure performance happens once we increase the number of RISs. Therefore, it is suitable for the implementation of low-power devices and short-range transmission associated with one RIS which helps to communicate to many devices with better coverage areas and reasonable cost.

4.1.2. Case $N \geqslant 2$

In this section, the PDF of X is given as [34]

$$f_{X^2}(x) = \frac{1}{2\sigma^2}\left(\frac{x}{\lambda}\right)^{-\frac{1}{4}} e^{-\frac{x+\lambda}{2\sigma^2}} I_{-\frac{1}{2}}\left(\frac{\sqrt{x\lambda}}{\sigma^2}\right), \tag{13}$$

where $\lambda = (\frac{N\pi}{4})^2$, $\sigma^2 = N(1-\frac{\pi^2}{16})^2$ and $I_v(\bullet)$ denotes the Bessel functions of the first class with order v [33]. Moreover, the PDF of γ_r with $r \in \{E, D\}$ can be expressed as

$$f_{\gamma_r}(x) = \frac{1}{2\sigma^2}\left(\frac{x}{\lambda}\right)^{-\frac{1}{4}}\left(\frac{1}{\bar{\gamma}_r}\right)^{\frac{3}{4}} e^{-\frac{x+\lambda\bar{\gamma}_r}{2\bar{\gamma}_r\sigma^2}} I_{-\frac{1}{2}}\left(\frac{\sqrt{x\lambda}}{\sqrt{\bar{\gamma}_r}\sigma^2}\right). \tag{14}$$

Based on [33, Eq. 8.445], we have

$$I_v(z) = \sum_{k=0}^{\infty} \frac{1}{k!\Gamma(v+k+1)}\left(\frac{z}{2}\right)^{v+2k}. \tag{15}$$

Then, we can rewrite (14) as

$$f_{\gamma_r}(x) = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\frac{\lambda}{2\sigma^2}} x^{k-\frac{1}{2}} e^{-\frac{x}{2\bar{\gamma}_r\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)\left(2\sigma^2\right)^{2k}\frac{1}{2}\left(\bar{\gamma}_r\right)^{k+\frac{1}{2}}}. \tag{16}$$

Therefore, the CDF of γ_j is written as

$$\begin{aligned} F_{\gamma_r}(x) &= 1 - Q_{\frac{1}{2}}\left(\frac{\sqrt{\lambda}}{\sigma}, \sqrt{\frac{x}{\bar{\gamma}_r\sigma^2}}\right) \\ &= \sum_{k=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k \gamma\left(k+\frac{1}{2}, \frac{x}{2\bar{\gamma}_r\sigma^2}\right), \end{aligned} \tag{17}$$

where $Q_m(a; b)$ is the Marcum Q-function [35] and $\gamma(\bullet, \bullet)$ is the gamma incomplete function [33].

Proposition 1. *The closed-form of SOP is given as (12), shown at the top of the next top page. It is noted that $W_{p,q}(\bullet)$ is the Whittaker function of the second kind [33] (see Eq. (18) given in Box I).*

Proof. See Appendix.

4.2. Approximation of secrecy outage probability at high SNR

In this section, in the high SNR regime, the SOP of (8) can be approximated as

$$\begin{aligned} SOP^{\infty} &\approx \Pr\left(\frac{\gamma_D}{\gamma_E} < \gamma_C\right) \\ &\approx \int_0^{\infty} F_{\gamma_D}(\gamma_C s) f_{\gamma_E}(s) ds. \end{aligned} \tag{19}$$

4.2.1. Case $N = 1$

In this case, by substituting (10) and (11) into (19), we can rewrite SOP^{∞} as

$$SOP^{\infty} \approx 1 - \frac{4}{\bar{\gamma}_E}\int_0^{\infty} \sqrt{\frac{\gamma_C s}{\bar{\gamma}_D}} K_0\left(2\sqrt{\frac{s}{\bar{\gamma}_E}}\right) K_1\left(2\sqrt{\frac{\gamma_C s}{\bar{\gamma}_D}}\right) ds. \tag{20}$$

With the help of [33, Eq. 6.576.4], SOP^{∞} can be obtained as

$$SOP^{\infty} \approx 1 - \frac{\bar{\gamma}_E\gamma_C}{2\bar{\gamma}_D} {}_2F_1\left(2, 2; 3; 1 - \frac{\gamma_C\bar{\gamma}_E}{\bar{\gamma}_D}\right). \tag{21}$$

4.2.2. Case $N \geqslant 2$

In this case, we can write SOP^{∞} with the help of (16) and (17) as

$$\begin{aligned} SOP^{\infty} &\approx \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{e^{-\frac{\lambda}{\sigma^2}}\lambda^{k+l}(1/\bar{\gamma}_E)^{l+\frac{1}{2}}}{k!l!\Gamma\left(k+\frac{1}{2}\right)\Gamma\left(l+\frac{1}{2}\right)} \\ &\times \int_0^{\infty} \frac{s^{l-\frac{1}{2}}}{\left(2\sigma^2\right)^{2l+k+\frac{1}{2}}} e^{-\frac{s}{2\bar{\gamma}_E\sigma^2}} \gamma\left(k+\frac{1}{2}, \frac{\gamma_C s}{2\bar{\gamma}_D\sigma^2}\right). \end{aligned} \tag{22}$$

Based on [33, Eq. 6.455.2], SOP^{∞} is given as

$$\begin{aligned} SOP^{\infty} &\approx \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{e^{-\frac{\lambda}{\sigma^2}}\Gamma(l+k+1)\left(\frac{\lambda}{2\sigma^2}\right)^{l+k}}{k!l!\Gamma\left(k+\frac{3}{2}\right)\Gamma\left(l+\frac{1}{2}\right)} \\ &\times \frac{{}_2F_1\left(1, k+l+1; k+\frac{3}{2}; \frac{\gamma_C\bar{\gamma}_E}{\gamma_C\bar{\gamma}_E+\bar{\gamma}_D}\right)}{\left(1+\frac{\bar{\gamma}_D}{\gamma_C\bar{\gamma}_E}\right)^{k+\frac{1}{2}}\left(1+\frac{\gamma_C\bar{\gamma}_E}{\bar{\gamma}_D}\right)^{l+\frac{1}{2}}}. \end{aligned} \tag{23}$$

Remark 1. Although expressions of these considered metrics are too complicated, but their secure performance mainly depends on the quality of channel and configuration of the RIS. As a result, main factors γ_D and γ_E need be controlled through RIS to achieve the expected secure performance. In the scope of this paper, we focus on determining particular values of these metrics for possible applications in the context of point-to-point IoT.

4.3. Secrecy capacity

Since PLS technique introduces new security approaches which rely on information theory fundamentals, our research direction is considerations on the secrecy capacity of the propagation channel. As a result, by examining secrecy capacity, we provide main metric to evaluate effectiveness of PLS. Specifically, the average secrecy capacity is defined as [36]

$$\begin{aligned} \bar{C}_S &= \mathbb{E}[C_S] \\ &= \underbrace{\mathbb{E}[\log_2(1+\gamma_D)]}_{C_D} - \underbrace{\mathbb{E}[\log_2(1+\gamma_E)]}_{C_E}. \end{aligned} \tag{24}$$

Then, the term C_r can be calculated as

$$C_r = \frac{1}{\ln(2)}\int_0^{\infty} \frac{1 - F_{\gamma_r}(x)}{1+x} dx. \tag{25}$$

4.3.1. Case $N = 1$

In this regard, putting (11) into (25) and after some variable substitutions and manipulations, C_D can be expressed as

$$C_D = \frac{1}{\ln(2)}\int_0^{\infty} \frac{1}{1+x}\sqrt{\frac{4x}{\bar{\gamma}_D}} K_1\left(\sqrt{\frac{4x}{\bar{\gamma}_D}}\right) dx. \tag{26}$$

Then, following the result reported in [33, 9.34.3], we get

$$C_D = \int_0^{\infty} \frac{G_{0,2}^{2,0}\left[\frac{x}{\bar{\gamma}_D}\middle|\begin{matrix}-\\1,0\end{matrix}\right]}{1+x} dx. \tag{27}$$

Using [33, Eq. 7.811.5], C_D can be obtained as

$$C_D = G_{1,3}^{3,1}\left[\frac{1}{\bar{\gamma}_D}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right]. \tag{28}$$

Similarly, the term C_E can be obtained as

$$C_E = G_{1,3}^{3,1}\left[\frac{1}{\bar{\gamma}_E}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right]. \tag{29}$$

$$SOP = \sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{\infty} \frac{\lambda^{k+l}(-1)^m e^{-\frac{\lambda}{\sigma^2}} e^{\frac{(\gamma_C-1)}{4\bar{\gamma}_E\gamma_C\sigma^2}} (\gamma_C-1)^{\frac{l+k+m}{2}} W_{\frac{k+m-l+2}{2},-\frac{k+m+l+1}{2}}\left(\frac{\gamma_C-1}{2\bar{\gamma}_E\gamma_C\sigma^2}\right)}{k!l!m!\left(k+m+\frac{1}{2}\right)\Gamma\left(k+\frac{1}{2}\right)\left(\sqrt{2\sigma^2}\right)^{3k+3l+m}(\bar{\gamma}_D)^{k+m+\frac{1}{2}}\left(\sqrt{\bar{\gamma}_E\gamma_C}\right)^{l-k-m-1}}. \quad (18)$$

Box I.

Finally, the closed-form of average secrecy capacity can be given by

$$\bar{C}_S = G_{1,3}^{3,1}\left[\frac{1}{\bar{\gamma}_D}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right] - G_{1,3}^{3,1}\left[\frac{1}{\bar{\gamma}_E}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right]. \quad (30)$$

4.3.2. Case $N \geqslant 2$

In this case, putting (17) into (25) we get C_D as

$$C_D = \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k \times\int_0^{\infty}\frac{\Gamma\left(\frac{1}{2}+k,\frac{x}{2\bar{\gamma}_D\sigma^2}\right)}{1+x}dx. \quad (31)$$

Based on [37, Eq. 5], we have

$$\Gamma(\alpha,x) = G_{1,2}^{2,0}\left(x\middle|\begin{matrix}1\\\alpha,0\end{matrix}\right). \quad (32)$$

Then, by substituting (32) into (31), we have

$$C_D = \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k \times\int_0^{\infty}\frac{1}{1+x}G_{1,2}^{2,0}\left(\frac{x}{2\bar{\gamma}_D\sigma^2}\middle|\begin{matrix}1\\\frac{1}{2}+k,0\end{matrix}\right)dx. \quad (33)$$

Similarly, the closed-form of C_D can be obtained as

$$C_D = \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k \times G_{2,3}^{3,1}\left(\begin{matrix}0,1\\0,\frac{1}{2}+k,0\end{matrix}\middle|\frac{1}{2\bar{\gamma}_D\sigma^2}\right). \quad (34)$$

Similarly, the closed-form of C_E can be obtained as

$$C_E = \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k \times G_{2,3}^{3,1}\left(\begin{matrix}0,1\\0,\frac{1}{2}+k,0\end{matrix}\middle|\frac{1}{2\bar{\gamma}_E\sigma^2}\right). \quad (35)$$

By putting (34) and (35) into (24), the closed-form of $\bar{C}_S$ can be obtained as (36), shown at the top of the next page.

$$\bar{C}_S = \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k G_{2,3}^{3,1}\left(\frac{1}{2\bar{\gamma}_D\sigma^2}\middle|\begin{matrix}0,1\\0,\frac{1}{2}+k,0\end{matrix}\right) - \sum_{k=0}^{\infty}\frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\Gamma\left(k+\frac{1}{2}\right)}\left(\frac{\lambda}{2\sigma^2}\right)^k G_{2,3}^{3,1}\left(\frac{1}{2\bar{\gamma}_E\sigma^2}\middle|\begin{matrix}0,1\\0,\frac{1}{2}+k,0\end{matrix}\right). \quad (36)$$

Remark 2. In general, the structures of 5G/6G networks or cellular based IoT systems are usually decentralized. In particular, devices may randomly connect in or leave the network at any time instants. For this circumstance, cryptographic key distribution and management become very challenging. As a result, such PLS technique along with performance analysis can be used to either perform secure data transmission directly or physical layer also generates the distribution of cryptography keys in the RIS-aided networks. Further, such PLS scheme together with careful management and implementation can be used as an additional level of protection on top of the existing security schemes. It is obviously predicted that our simulations presented in the next section aim to find relevant system parameters to guarantee security of such RIS-aided system.

Table 3
Table of parameters.

The average SNR	$\bar{\gamma}_E = -10$ dB
The target secrecy rate	$C_{th} = 1$
The normalized distances	$d_R = d_D = d_E = 1$
The path-loss coefficient	$\beta = 2$

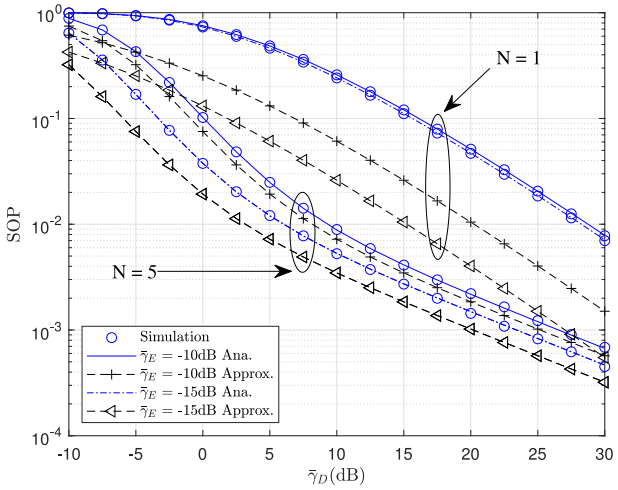

Fig. 2. The SOP versus $\bar{\gamma}_D$ varying $\bar{\gamma}_E$.

5. Numerical simulation

We conduct numerical simulation and provide detailed explanations regarding the mathematical results. Regarding Monte-Carlo simulations, 10^6 iterations are performed to verify the exactness of expressions derived in the paper. The main parameters are introduced in Table 3. In all figures, we denote two methods of simulations, i.e. "simulation" or "Sim". for Monte-Carlo runs and "Analytical" or "Ana". for runs relying on analytical expressions.

5.1. The impact of levels of eavesdropping signal

We start our investigation in terms of numerical results by comparing the secure outage behavior of RIS-aided system with different setups related to the number of RIS elements. In Fig. 2,

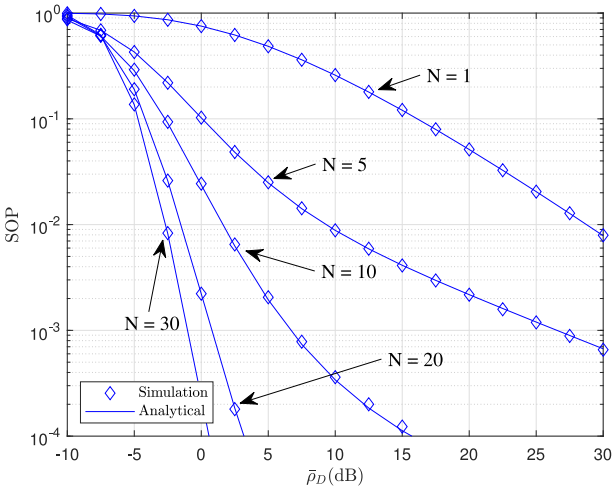

Fig. 3. The SOP versus $\bar{\gamma}_D$ varying the number of RIS elements N.

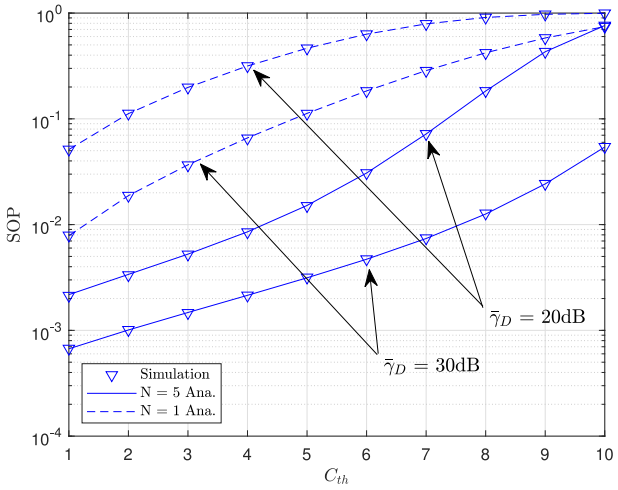

Fig. 4. The SOP versus C_{th} varying $\bar{\gamma}_D$.

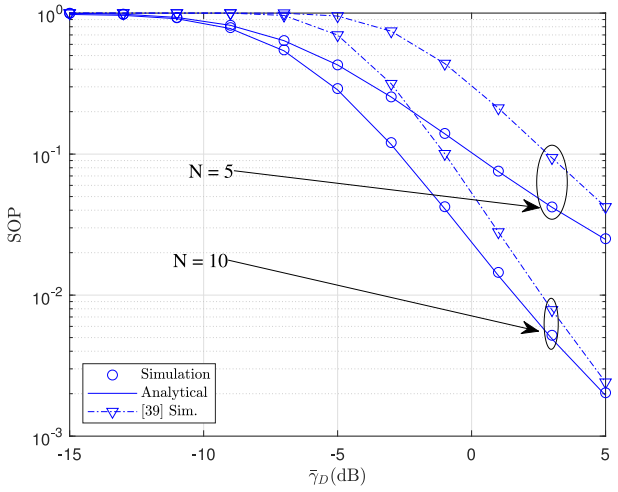

Fig. 5. The SOP versus $\bar{\gamma}_D$ comparison with [30].

we can see clearly that values of transmitted SNR $\bar{\gamma}_D$ at the AP contributes mainly to improve SOP performance, especially SOP is very small at $\bar{\gamma}_D = 30$. We conduct Monte-Carlo and analytical simulations which exhibit precisely that these curves are matched very tightly. As a result, such matching curves confirm the high accurate computation of SOP metric in this study. The main observation is that lower level of eavesdropping signal which leads to better SOP performance. At particular point $\bar{\gamma}_E = -15$, we can find the best SOP case. For the approximation scenario where we clearly look at the gap among exact and approximated curves in term of SOP performance. As can be seen clearly, for the case of $N = 5$, the secrecy outcomes of two methods of computation for SOP metric are very close. The main reason for such observation is that the reflective link associated with RIS may even strengthen the signal strength of second hop transmission, if the reflective phase shift is not properly designed. We can conclude that the higher number of RIS elements make significant improvement of reflecting signals from RIS to IoT devices.

5.2. The impact of the number of RIS elements

For satisfy low-cost in hardware design, the literature reported detailed performance analysis of RIS-aided systems over some kinds of fading channels [10], taking into account of the number of RIS metasurface elements. Once can conclude from the closed-form expressions of both the ergodic capacity and outage probability that more RIS elements lead to significant improvement. By exploiting simplified expressions are obtained in the approximate regime as [38], the findings suggested that the RIS can provide an effective SNR gain of N. However, higher cost of RIS design is not necessary for some applications in IoT systems.

As can be seen from Fig. 3, the performances of RIS-aided system can be enhanced by increasing the average SNR at the AP $\bar{\gamma}_D$. More importantly, this figure shows how the number of RIS elements can boost secure performance. In the best scenario, when $N = 30$, the value of the SOP has surge reduction. In other words, trade-off of the number of RIS elements and cost of RIS design should be further studied.

We can see limitation of secure performance at high value of C_{th}, shown as Fig. 4. It can be concluded from expressions of SOP metric that higher C_{th} leads to degradation in term of SOP. This can be explained that C_{th} limit average rate, then the corresponding SOP can be adjusted. As the worst scenario, when $N = 1$ and $\bar{\gamma}_D = 20$ dB, the value of the SOP equals exactly one. In this case, higher required data rate would be main reason of degraded secure performance. As alternative way, design a RIS with high metasurface N can improve SOP performance instead of increasing threshold rate C_{th}.

Fig. 5, we plot the SOP curves for different N when we compare this work with similar study reported in [30]. To simplify simulation, we provide SOP performance of the work in [30] by running Monte-Carlo method. As can be seen from Fig. 5, it is shown that N has a great impact on the system performance. The SOP becomes higher when N increases. At specific point $\bar{\gamma}_D = 5$ and $N = 10$, SOP in our system outperforms that reported in [30] around 5.2%. For the case of $N = 5$ such improvement could be 10%.

5.3. The considerations $\bar{\gamma}_D$ and N on secrecy capacity

Fig. 6 shows the secrecy capacities versus $\bar{\gamma}_D$. In this circumstance, the number of reflector elements N is recognized as main factor affecting secure system performance metric. From Fig. 6, it is observed that the gap between the curves of the three cases of N increases when N increases. It can be explained that RIS provides more degree of freedom if we set high RIS reflecting elements which make influence to weak signal and strong signal associated with the wiretap and main channel, respectively, and thus obtains the high gains.

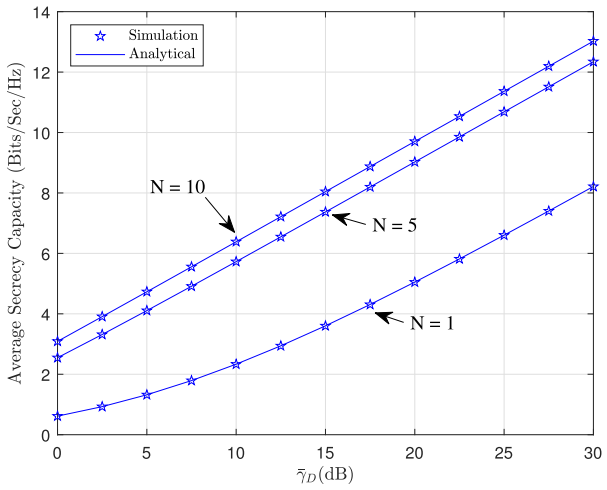

Fig. 6. The average secrecy capacity versus $\bar{\gamma}_D$ varying N.

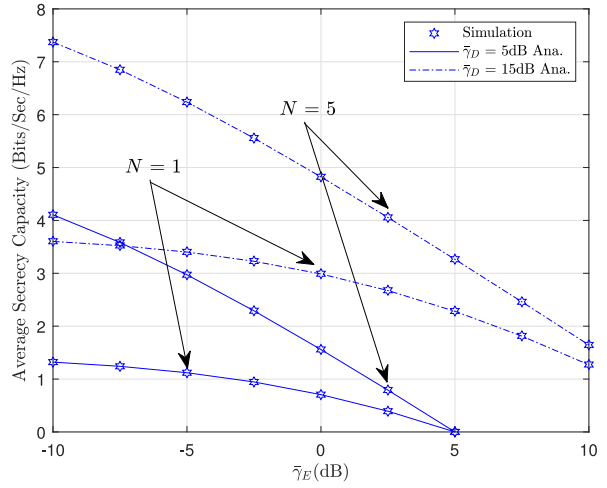

Fig. 7. The average secrecy capacity versus $\bar{\gamma}_E$ varying $\bar{\gamma}_D$.

Fig. 7 shows the secrecy capacity versus the average $\bar{\gamma}_E$ with two cases of the number of RIS's reflecting units in the cases of $\bar{\gamma}_D = 5$ (dB) and $\bar{\gamma}_D = 15$ (dB). The fading factors are set identical to those in previous figures. By increasing N at the RIS, the secrecy capacity achieved in the proposed RIS increases significantly and this situation makes dominant for legitimate user. Furthermore, the performance gap between two values of N when we fixed indicator of $\bar{\gamma}_D$ and the worse secure performance becomes more pronounced at high level of eavesdropper's signal.

6. Conclusion

In this paper, we have studied PLS in point-to-point RIS-aided IoT systems. We investigated the secure outage probability and average secrecy capacity for several scenarios of the RIS under the presence of an eavesdropper. The results showed that the RIS with a large number of reflecting elements provides higher security outcomes for all the considered scenarios including varying the average SNR of the eavesdropper and the legitimate IoT device, changing the transmit source power from the BS, and the threshold target rates. In particular, $N = 10$, $C_{th} = 1$ (bps/Hz) are a possible set of main parameters to achieve reasonable system performance metrics including SOP and average secrecy capacity. Further, at a high SNR at the AP, we can improve SOP performance by 10% compared with recent studies [30]. As a possible future extension of this article, we can also consider non-orthogonal multiple access design which get more benefits from the main advantages of RIS. For instance, we can validate performance gaps among IoT devices (far and near devices). In addition, cognitive radio and wireless power transfer are recommended as two approaches to further improve both energy efficiency secure performance metrics for RIS-aided IoT systems.

CRediT authorship contribution statement

Dinh-Thuan Do: Conceptualization, Methodology, Partly calculating performance metrics and writing. **Anh-Tu Le:** Coding and partly calculating performance metrics. **Nhat-Duy Xuan Ha:** Coding and partly calculating performance metrics. **Nhu-Ngoc Dao:** Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

Putting (8) and (9) into (11), we have

$$SOP = \int_0^\infty F_{\gamma_D}(\gamma_C + \gamma_C s - 1) f_{\gamma_E}(s)\, ds$$
$$= \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{\lambda^{k+l} e^{-\frac{\lambda}{\sigma^2}} (1/\bar{\gamma}_E)^{l+\frac{1}{2}}}{k!l!\Gamma\left(k+\frac{1}{2}\right)\Gamma\left(l+\frac{1}{2}\right)} \left(\frac{1}{2\sigma^2}\right)^{k+2l+\frac{1}{2}} \tag{37}$$
$$\times \int_0^\infty s^{l-\frac{1}{2}} e^{-\frac{s}{2\bar{\gamma}_E\sigma^2}} \gamma\left(k+\frac{1}{2}, \frac{\gamma_C+\gamma_C s-1}{2\bar{\gamma}_D\sigma^2}\right) ds.$$

Based on [33, Eq. 8.354], we have

$$\gamma(\alpha, x) = \sum_{n=0}^{\infty} \frac{(-1)^n x^{\alpha+n}}{n!(\alpha+n)}. \tag{38}$$

With the help of (38) and (39), the expected expression of SOP is rewritten as

$$SOP = \sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{\infty} \frac{\lambda^{k+l}(-1)^m e^{-\frac{\lambda}{\sigma^2}}}{k!l!m!\left(k+m+\frac{1}{2}\right)}$$
$$\times \left(\frac{1}{2\sigma^2}\right)^{2k+2l+m+1} \left(\frac{1}{\bar{\gamma}_D}\right)^{k+m+\frac{1}{2}} \left(\frac{1}{\bar{\gamma}_E}\right)^{l+\frac{1}{2}} \tag{39}$$
$$\times \int_0^\infty \frac{s^{l-\frac{1}{2}}(\gamma_C-1+\gamma_C s)^{k+m+\frac{1}{2}} e^{-\frac{s}{2\bar{\gamma}_E\sigma^2}} ds}{\Gamma\left(l+\frac{1}{2}\right)\Gamma\left(k+\frac{1}{2}\right)}.$$

Putting $t = \gamma_C - 1 + \gamma_C s$ and after some variable substitutions and manipulations, we have

$$SOP = \sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{\infty} \frac{\lambda^{k+l}(-1)^m e^{-\frac{\lambda}{\sigma^2}} e^{\frac{(\gamma_C-1)}{2\bar{\gamma}_E\gamma_C\sigma^2}}}{k!l!m!\left(k+m+\frac{1}{2}\right)\Gamma\left(l+\frac{1}{2}\right)}$$
$$\times \frac{\left(1/2\sigma^2\right)^{2k+2l+m+1}(1/\gamma_C)^{l+\frac{1}{2}}}{\Gamma\left(k+\frac{1}{2}\right)(\bar{\gamma}_D)^{k+m+\frac{1}{2}}(\bar{\gamma}_E)^{l+\frac{1}{2}}} \tag{40}$$
$$\times \int_{\gamma_C-1}^\infty (t-(\gamma_C-1))^{l-\frac{1}{2}} t^{k+m+\frac{1}{2}} e^{-\frac{t}{2\bar{\gamma}_E\gamma_C\sigma^2}} dt.$$

Based on [33, Eq 3.383.4] and after some algebraic manipulations, final result can be obtained.

The proof is completed.

References

[1] A. Ghasempour, Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges, Invent. J. 4 (1) (2019) 1–12.

[2] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, K. Zeng, Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities, IEEE Internet Things J. 6 (5) (2019) 8169–8181.

[3] Z. Deng, Q. Li, Q. Zhang, L. Yang, J. Qin, Beamforming design for physical layer security in a two-way cognitive radio IoT network with SWIPT, IEEE Internet Things J. 6 (6) (2019) 10786–10798.

[4] Heejung Yu, Il-Gu Lee, Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay, Future Gener. Comput. Syst. 102 (2020) 611–618.

[5] X. Sun, D.W.K. Ng, Z. Ding, Y. Xu, Z. Zhong, Physical layer security in UAV systems: Challenges and opportunities, IEEE Wirel. Commun. 26 (5) (2019) 40–47.

[6] X. Wang, W. Feng, Y. Chen, N. Ge, UAV swarm-enabled aerial CoMP: A physical layer security perspective, IEEE Access 7 (2019) 120901-120916.

[7] Y. Zhou, et al., Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location, IEEE Trans. Veh. Technol. 67 (11) (2018) 11280–11284.

[8] F. Liu, J. Li, S. Li, Y. Liu, Physical layer security of full-duplex two-way AF relaying networks with optimal relay selection, in: 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6.

[9] M.H. Khoshafa, T.M.N. Ngatched, M.H. Ahmed, On the physical layer security of underlay relay-aided device-to-device communications, IEEE Trans. Veh. Technol. 69 (7) (2020) 7609–7621.

[10] Q. Wu, R. Zhang, Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network, IEEE Commun. Mag. 58 (1) (2020) 106–112.

[11] S. Gong, et al., Towards smart radio environment for wireless communications via intelligent reflecting surfaces: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020) http://dx.doi.org/10.1109/COMST.2020.3004197.

[12] X. Guan, Q. Wu, R. Zhang, Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not? IEEE Wirel. Commun. Lett. 23 (9) (2019) 1488–1492.

[13] H. Shen, W. Xu, S. Gong, Z. He, C. Zhao, Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications, IEEE Commun. Lett. 23 (9) (2019) 1488–1492.

[14] Z. Chu, W. Hao, P. Xiao, J. Shi, Intelligent reflecting surface aided multi-antenna secure transmission, IEEE Wirel. Commun. Lett. 9 (1) (2020) 108–112.

[15] X. Yu, D. Xu, Y. Sun, D.W.K. Ng, R. Schober, Robust and secure wireless communications via intelligent reflecting surfaces, IEEE J. Sel. Areas Commun. 38 (11) (2020) 2637–2652.

[16] K. Feng, X. Li, Y. Han, S. Jin, Y. Chen, Physical layer security enhancement exploiting intelligent reflecting surface, IEEE Commun. Lett. http://dx.doi.org/10.1109/LCOMM.2020.3042344.

[17] M. Cui, G. Zhang, R. Zhang, Secure wireless communication via intelligent reflecting surface, IEEE Wirel. Commun. Lett. 8 (5) (2019) 1410–1414.

[18] M. Wijewardena, T. Samarasinghe, K.T. Hemachandra, S. Atapattu, J.S. Evans, Physical layer security for intelligent reflecting surface assisted two–way communications, IEEE Commun. Lett., http://dx.doi.org/10.1109/LCOMM.2021.3068102.

[19] H. Shen, W. Xu, S. Gong, Z. He, C. Zhao, Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications, IEEE Commun. Lett. 23 (9) (2019) 1488–1492.

[20] X. Yu, D. Xu, R. Schober, Enabling secure wireless communications via intelligent reflecting surfaces, in: 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1–6.

[21] W. Jiang, Y. Zhang, J. Wu, W. Feng, Y. Jin, Intelligent reflecting surface assisted secure wireless communications with multiple transmit and multiple-receive antennas, 2019, [Online]. Available: https://arxiv.org/abs/2001.08963.

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

[23] A. Pandey, S. Yadav, Dinh-Thuan. Do, R. Kharel, Secrecy performance of cooperative cognitive AF relaying networks with direct links over mixed rayleigh and double-rayleigh fading channels, IEEE Trans. Veh. Technol. http://dx.doi.org/10.1109/TVT.2020.3034729.

[24] R. Nakai, S. Sugiura, Physical layer security in buffer-state based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming, IEEE Trans. Inf. Forensics Secur. 14 (2) (2019) 431–444.

[25] Q. Chen, M. Li, X. Yang, R. Alturki, M.D. Alshehri, F. Khan, Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks, IEEE Access 9 (2021) 42583–42592.

[26] J. Li, A.P. Petropulu, S. Weber, On cooperative relaying schemes for wireless physical layer security, IEEE Trans. Signal Process. 59 (10) (2011) 4985–4997.

[27] Z. Zhu, N. Wang, W. Hao, Z. Wang, I. Lee, Robust beamforming designs in secure MIMO SWIPT IoT networks with a nonlinear channel model, IEEE Internet Things J. 8 (3) (2021) 1702–1715.

[28] L. Hu, et al., Cooperative jamming for physical layer security enhancement in Internet of Things, IEEE Internet Things J. 5 (1) (2018) 219–228.

[29] W. Huang, Y. Zeng, Y. Huang, Achievable rate region of MISO interference channel aided by intelligent reflecting surface, IEEE Trans. Veh. Technol. http://dx.doi.org/10.1109/TVT.2020.3038385.

[30] L. Yang, J. Yang, W. Xie, M.O. Hasna, T. Tsiftsis, M.D. Renzo, Secrecy performance analysis of RIS-aided wireless communication systems, IEEE Trans. Veh. Technol. 69 (10) (2020) 12296–12300.

[31] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inform. Theory 54 (6) (2008) 2515–2534.

[32] S. Atapattu, R. Fan, P. Dharmawansa, G. Wang, J. Evans, T.A. Tsiftsis, Reconfigurable intelligent surface assisted two–way communications: Performance analysis and optimization, IEEE Trans. Commun. 68 (10) (2020) 6552–6567.

[33] I.S. Gradshteyn, I.M. Ryzhik, Table of Integrals, Series, and Products, seventh ed., Academic, San Diego, CA, USA, 2007.

[34] L. Yang, Y. Yang, M.O. Hasna, M.-S. Alouini, Coverage, probability of SNR gain, and DOR analysis of RIS-aided communication systems, IEEE Wirel. Commun. Lett. 9 (8) (2020) 1268–1272.

[35] V.M. Kapinas, S.K. Mihos, G.K. Karagiannidis, On the monotonicity of the meneralized Marcum and Nuttall Q-functions, IEEE Trans. Inform. Theory 55 (8) (2009) 3701–3710.

[36] O.S. Badarneh, P.C. Sofotasios, S. Muhaidat, S.L. Cotton, K. Rabie, N. Al-Dhahir, On the secrecy capacity of Fisher-Snedecor F fading channels, in: 14th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob), Oct. 2018, pp. 102–107.

[37] S. Kumar, Exact evaluations of some Meijer G-functions and probability of all eigenvalues real for the product of two Gaussian matrices, J. Phys. A (2015).

[38] A. Hemanth, K. Umamaheswari, A.C. Pogaku, D.-T. Do, B.M. Lee, Outage performance analysis of reconfigurable intelligent surfaces-aided NOMA under presence of hardware impairment, IEEE Access 8 (2020) 212156-212165.

Dinh-Thuan Do (Senior Member, IEEE) received the B.S., M.Eng., and Ph.D. degrees from Vietnam National University (VNU-HCMC), in 2003, 2007, and 2013, respectively, all in communications engineering. Prior to joining The University of Texas at Austin, UAS, he was an assistant professor at Ton Duc Thang University and a Senior Engineer with VinaPhone Mobile Network. His research interests include signal processing in wireless communications networks, NOMA, full-duplex transmission, and energy harvesting. Dr. Thuan was a recipient of Golden Globe Award from Vietnam Ministry of Science and Technology in 2015 (Top 10 most excellent scientist nationwide). He is currently serving as an Editor of COMPUTER COMMUNICATIONS (Elservier), an Associate Editor of EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING (Springer), ELECTRONICS, ICT EXPRESS, and KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. He was a Lead Guest Editor of the Special Issue "Recent Advances for 5G: Emerging Scheme of NOMA in Cognitive Radio and Satellite Communications" in ELECTRONICS in 2019. He is also serving as Guest Editor of a Special Issue on "Massive sensors data fusion for health-care informatics" in ANNALS OF TELECOMMUNICATIONS (Springer) in 2020, as a Guest Editor of a Special Issue on "Power Domain Based Multiple Access Techniques in Sensor Networks" in INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS (IJDSN) in 2020 and a Guest Editor of a Special Issue on "UAV-enabled B5G/6G Networks: Emerging Trends and Challenges" in PHYSICAL COMMUNICATION (Elservier), 2020.His publications include over 100 SCIE/SCI-indexed journal articles, over 60 SCOPUS-indexed journal articles and over 50 international conference papers. He is sole author in one textbook, one edited book and six book chapters.

Anh-Tu Le was born in LAM DONG, Vietnam, in 1997. He is pursuing the Ph.D. degree in communication and information system fin field of Wireless Communication. He is currently a Research Assistant with the WICOM lab which was led by Dr. Thuan. He has authored or co-authored over 5 technical papers published in peer-reviewed international journals. His research interests include the wireless channel modeling, NOMA, cognitive radio and MIMO.

Nhat-Duy Xuan Ha was born in GIA LAI, Vietnam, in 1996. He is pursuing the Ph.D. degree in communication and information system in field of Wireless Communication. He is currently a Research Assistant with the WICOM lab which was led by Dr. Thuan. His research interests include the wireless communications, NOMA, cognitive radio, satellite systems.

Nhu-Ngoc Dao (Member, IEEE) is an Assistant Professor at the Department of Computer Science and Engineering, Sejong University, Seoul, Republic of Korea. He received his M.S. and Ph.D. degrees in computer science at the School of Computer Science and Engineering, Chung-Ang University, Seoul, Republic of Korea, in 2016 and 2019, respectively. He received the B.S. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology, Hanoi, Viet Nam, in 2009. Prior to joining the Sejong University, he was a postdoc researcher at the Institute of Computer Science, University of Bern, Switzerland from 2019 to 2020. His research interests include network softwarization, mobile cloudization, intelligent system, and the Internet of Things.