sensors

MDPI

Communication

Physical-Layer Security Improvement with Reconfigurable Intelligent Surfaces for 6G Wireless Communication Systems

Janghyuk Youn, Woong Son and Bang Chul Jung *

Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea; jhyoon@o.cnu.ac.kr (J.Y.); woongson@cnu.ac.kr (W.S.)
* Correspondence: bcjung@cnu.ac.kr; Tel.: +82-42-821-6580

Abstract: Recently, reconfigurable intelligent surfaces (RISs) have received much interest from both academia and industry due to their flexibility and cost-effectiveness in adjusting the phase and amplitude of wireless signals with low-cost passive reflecting elements. In particular, many RIS-aided techniques have been proposed to improve both data rate and energy efficiency for 6G wireless communication systems. In this paper, we propose a novel RIS-based channel randomization (RCR) technique for improving physical-layer security (PLS) for a time-division duplex (TDD) downlink cellular wire-tap network which consists of a single base station (BS) with multiple antennas, multiple legitimate pieces of user equipment (UE), multiple eavesdroppers (EVEs), and multiple RISs. We assume that only a line-of-sight (LOS) channel exists among the BS, the RISs, and the UE due to propagation characteristics of tera-hertz (THz) spectrum bands that may be used in 6G wireless communication systems. In the proposed technique, each RIS first pseudo-randomly generates multiple reflection matrices and utilizes them for both pilot signal duration (PSD) in uplink and data transmission duration (DTD) in downlink. Then, the BS estimates wireless channels of UE with reflection matrices of all RISs and selects the UE that has the best secrecy rate for each reflection matrix generated. It is shown herein that the proposed technique outperforms the conventional techniques in terms of achievable secrecy rates.

Keywords: physical-layer security; reconfigurable intelligent surface; intelligent reflecting surface; secure communication; passive eavesdropper; 6G wireless communication system; tera-hertz spectrum

Citation: Youn, J.; Son, W.; Jung, B.C. Physical-Layer Security Improvement with Reconfigurable Intelligent Surfaces for 6G Wireless Communication Systems. *Sensors* **2021**, *21*, 1439. https://doi.org/10.3390/s21041439

Academic Editor: Adrian Bekasiewicz
Received: 22 January 2021
Accepted: 17 February 2021
Published: 19 February 2021

1. Introduction

Reconfigurable intelligent surfaces (RISs) or intelligent reflecting surfaces (IRSs) have been proposed to achieve high spectral and energy efficiency for future 6G wireless communication systems [1–4]. An RIS consists of a large number of passive elements, each of which can independently change the received signal and reflect the altered signal. For the passive elements that can reflect, conventional reflect-arrays, liquid crystal surfaces, or software-defined meta-surfaces can be applied [5]. In particular, millimeter-wave (mmWave) and tera-hertz (THz) communication are known to be well-compatible with the RISs for line-of-sight (LOS) environments, since mmWave and THz communications suffer from significant path-loss in general. There exist several studies related to the RIS in LOS environments for mmWave and THz communications. For example, an RIS-aided joint optimization technique of the transmit beam forming at the access point (AP) and passive phase-shift at the RIS was investigated to enhance the energy efficiency at the AP in RIS-aided multi-user multiple-input single-output (MISO) communication systems [6]. An RIS-based phase-shift technique for effective ranking with a singular value of the RIS-augmented channel maximization was investigated in RIS-aided multi-user single-input multiple-output (SIMO) communication systems [7]. In addition, RIS was applied to a mobile edge computing system for maximizing the sum of computational bits, since the benefits of RISs can be

exploited to enhance computing performance [8]. Moreover, it was shown that the RISs can improve the ranks of LOS MIMO communication systems [9].

Meanwhile, physical-layer security (PLS) has received considerable attention from both academia and industry [10]. Many studies have been performed to enhance PLS for future wireless networks, such as massive MIMO, non-orthogonal multiple access (NOMA), Internet of Things (IoT) networks, and mmWave and THz communications [11–13]. The eavesdropping attack scenario in which a malicious device attempts to overhear a private message between legitimate devices is constantly being considered as an important security issue in the literature [14]. Eavesdropping scenarios with the PLS can be classified into three scenarios: passive, active, and potential eavesdropping scenarios [15–23]. A passive eavesdropper (EVE) always attempts to overhear the private message and does not take any other proactive actions [15–19]. By contrast, an active EVE not only attempts to overhear the private message, but also induces some malfunction, such as artificial noise, a jamming attack, pilot contamination, or fake information feedback [16,17]. The concept of the potential EVE was introduced in [20–23]. The term potential is used in the sense that the EVEs may operate as legitimate devices in some instances. For example, in multi-user uplink cellular networks, all unscheduled legitimate users in a certain cell are defined as potential EVEs in [21], and some of the unscheduled users in a certain cell are defined as potential EVEs in [22]. Furthermore, in multi-user downlink cellular networks, potential EVEs can attempt to overhear legitimate communications of other cellphones or participate in their own legitimate communications [20,23].

Recently, it was shown that the performance of PLS can be improved by adding RISs to wireless communication systems [24–32]. These techniques have been proposed to improve the secrecy rate by maximizing the legitimate channel gain and minimizing the eavesdropping channel gain for private message transmission through the legitimate link. Furthermore, joint transmit beamforming and reflecting beamforming optimization with artificial noise (AN) or jamming signals have been proposed for PLS enhancement in various wireless networks [33–39]. These techniques aim to maximize the signal to interference-plus-noise ratio (SINR) for a legitimate user and to minimize SINR for the EVE by transmitting a signal that combines the private message and AN. There have been several studies that considered legitimate links which were reflected only on RISs due to some obstacle [29,30,33], and some giving imperfect channel state information (CSI) to EVEs [35,38]. In addition, the multiple RIS-based joint transmit beamforming and AN optimization technique considering a potential eavesdropping attack scenario for PLS enhancement was proposed in [36]. However, in the literature, most studies considered iterative heuristic or complex algorithms for optimization, which require significant signaling overheads among the BS, RISs, and user equipment (UE), and if necessary, EVEs. Thus, a practical PLS improvement technique with RISs that does not involve a significant signaling overhead is required.

In this paper, we propose a novel RIS-based channel randomization (RCR) technique for improving PLS for a time-division duplex (TDD) downlink cellular wire-tap network consisting of a single BS, multiple legitimate pieces of UE, multiple passive EVEs, and multiple RISs. Each RIS pseudo-randomly generates multiple reflection matrices and utilizes them for pilot signal duration (PSD) in uplink and data transmission duration (DTD) in downlink. The BS estimates all wireless channels to the UE, including reflected wireless channels at IRSs, and selects the UE which can be achieve the best secrecy rate for each reflection matrix generated. As a result, our main contributions can be summarized as follows:

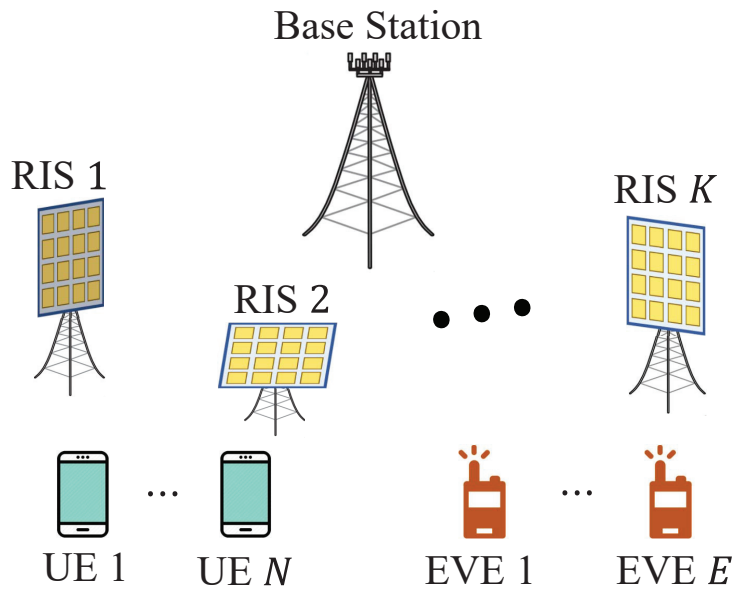
- We propose an RCR technique that repeats some random channel by repeating a certain number of reflecting matrices of the RIS. With the RCR technique, we can design a repeating random communication channel, possibly even in a short enough time that the communication channel will not be changed.
- Based on the RCR technique, user scheduling for each random channel was performed to maximize the secrecy rate. It was shown that the proposed RCR-based scheduling

technique can achieve better performance than the network without any RIS and than a random scheduling technique.

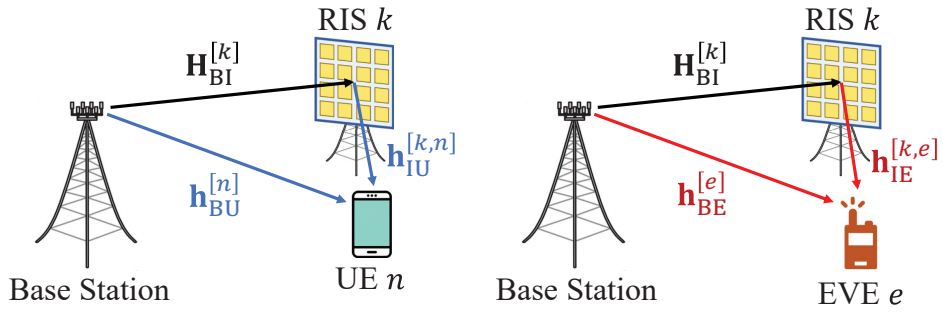
The rest of paper is composed as follows. In Section 2, the considered system model is described. Then the overall procedure of proposed RCR technique is explained in Section 3. The numerical results are shown in Section 4 and the proposed RCR technique is compared with reference techniques. Finally, the conclusion of this paper is written in Section 5.

2. System and Channel Model

In Figure 1a, the considered system in this paper is described, which consists of a BS, multiple RISs (K), multiple pieces of UE (N), and multiple EVEs, E. Note that EVE is the potential EVE—one of the pieces of user equipment outside of the cell, which transmits a pilot signal for its own communication. However, here, EVEs can overhear the other pieces of UE's communications and decode the private messages which are transmitted for other legitimate UE. With this assumption, the BS can acquire the CSI with EVEs by receiving the pilot signal from EVEs. Moreover, the BS is equipped with transmit antennas (M), RISs are equipped with multiple passive reflecting elements (L), and all UE and all EVEs are equipped with a single receiving antenna. For the BS and RISs, the uniform linear array (ULA) structure is adopted for transmitting antennas and passive reflecting elements, respectively.



(**a**) RIS-based communication system model.



(**b**) Communication channels in legitimate and eavesdropping channels in the model system.

Figure 1. RIS-based communication model and channel model.

As described in Figure 1b, the communication channels from the BS to the k-th RIS, from the BS to the n-th piece of UE, and from the BS to the e-th EVE are represented by $\mathbf{H}_{\mathsf{BI}}^{[k]}$, $\mathbf{h}_{\mathsf{BU}}^{[n]}$, and $\mathbf{h}_{\mathsf{BE}}^{[e]}$, respectively. In addition, $\mathbf{h}_{\mathsf{IU}}^{[n]}$ and $\mathbf{h}_{\mathsf{IE}}^{[e]}$ respectively denote the communication channel from the RIS to the n-th piece of UE and from the RIS to the e-th EVE. We assume that all channels in the considered system are LOS channels, since an extremely high frequency band will be utilized in 6G. Hence, all communication channels are defined as follows.

$$\begin{aligned}
\mathbf{H}_{\mathsf{BI}}^{[k]} &= \sqrt{ML}\mathbf{a}_L\left(\theta_{\mathsf{BI,R}}^{[k]}\right)\mathbf{a}_M\left(\theta_{\mathsf{BI,T}}^{[k]}\right)^H, \\
\mathbf{h}_{\mathsf{BU}}^{[n]} &= \sqrt{M}\mathbf{a}_M\left(\theta_{\mathsf{BU,T}}^{[n]}\right)^H, \\
\mathbf{h}_{\mathsf{BE}}^{[e]} &= \sqrt{M}\mathbf{a}_M\left(\theta_{\mathsf{BE,T}}^{[e]}\right)^H, \\
\mathbf{h}_{\mathsf{IU}}^{[n]} &= \sqrt{L}\mathbf{a}_L\left(\theta_{\mathsf{IU,T}}^{[n]}\right)^H, \\
\mathbf{h}_{\mathsf{IE}}^{[e]} &= \sqrt{L}\mathbf{a}_L\left(\theta_{\mathsf{IE,T}}^{[e]}\right)^H,
\end{aligned} \tag{1}$$

where $\mathbf{a}_X(\theta) = \left[1, e^{-j\pi\theta}, \cdots, e^{-j\pi(X-1)\theta}\right]^T$ is a steering vector for a given number of antennas, X is the angle of arrival or angle of departure, and θ is half of the wavelength antenna spacing. Moreover, $\theta_{\mathsf{X,T}}^{[x]}$ and $\theta_{\mathsf{X,R}}^{[x]}$ represent angle of departure and angle of arrival for corresponding channel $\mathbf{H}_{\mathsf{X}}^{[x]}$ or $\mathbf{h}_{\mathsf{X}}^{[x]}$, respectively. In addition, we assume that all LOS channels do not change in the course of a single transmission, but change after transmission ends.

3. The RIS-Based Channel Randomization Technique for Secure Communication

In this section, we describe the overall procedure of the proposed RIS-based channel randomization (RCR) technique for secure communication. Conceptually, RISs in the proposed technique repeat the reflection matrix upon pilot signal transmission and data signal transmission; reflection matrices are randomly generated.

First of all, we separate the communication duration into a pilot signal duration (PSD) and data transmission duration (DTD). PSD has T time slots and DTD has βT time slots, where β is a natural number. Before the transmission procedure starts, each k-th RIS generates T random reflection matrices, which correspond to T time slots in PSD, as shown in Figure 2. Then, the reflection matrix of the k-th RIS that corresponds to the t-th time slot is denoted as $\mathbf{G}_{k,t}$, and the set of reflection matrices for PSD is derived as follows.

$$\mathcal{G}_k = \left\{\mathbf{G}_{k,1}, \mathbf{G}_{k,2}, \cdots, \mathbf{G}_{k,T}\right\}, \tag{2}$$

where the reflection matrix $\mathbf{G}_{k,t}$ is defined as follows

$$\mathbf{G}_{k,t} = \begin{bmatrix} e^{j\phi_{k,t}^{[1]}} & 0 & \cdots & 0 \\ 0 & e^{j\phi_{k,t}^{[2]}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{j\phi_{k,t}^{[L]}} \end{bmatrix}, \tag{3}$$

where $\phi_{k,t}^{[l]}$ represents the random phase of the l-th passive reflecting element in the k-th RIS at the t-th time slot.

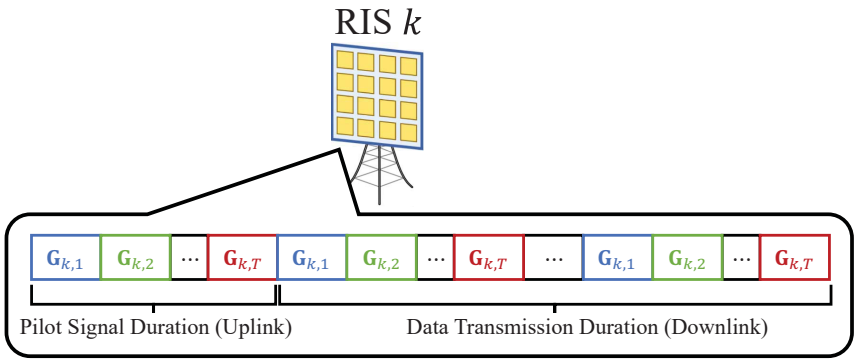


Figure 2. RIS reflection matrix shifting in pilot signal duration and data signal duration.

After the reflection matrix set is generated, all UE and EVEs transmit pilot signal to the BS during all time slots over the PSD. Then, the BS acquires all CSI between itself and UE or EVEs; thus, the CSI acquired with the n-th UE and the e-th EVE in t-th time slot can be derived as follows:

$$\begin{aligned} \mathbf{h}_{\mathsf{U}}^{[n,t]} &= \mathbf{h}_{\mathsf{BU}}^{[n]} + \sum_{k=1}^{K} \mathbf{h}_{\mathsf{IU}}^{[k,n]} \mathbf{G}_{k,t} \mathbf{H}_{\mathsf{BI}}^{[k]}, \\ \mathbf{h}_{\mathsf{E}}^{[e,t]} &= \mathbf{h}_{\mathsf{BE}}^{[e]} + \sum_{k=1}^{K} \mathbf{h}_{\mathsf{IE}}^{[k,e]} \mathbf{G}_{k,t} \mathbf{H}_{\mathsf{BI}}^{[k]}, \end{aligned} \tag{4}$$

respectively. Note that the reflection matrices of the RIS are the only time varying parameter of the channel between the BS and the UE or EVE, since we assume there are only LOS channels between nodes. Now, based on acquired CSI, BS allocates UE to each t-th time slot based on the following allocation metric:

$$n_t = \underset{n}{\operatorname{argmax}} \frac{\left| \mathbf{h}_{\mathsf{U}}^{[n,t]} \right|^2}{\max\limits_{e} \left| \mathbf{h}_{\mathsf{E}}^{[e,t]} \right|}, \tag{5}$$

where n_t is the UE index that is allocated to the t-th time slot, and this allocation metric makes the BS allocate each n-th UE to the specific time slot that should achieve the best secrecy rate. In addition, since the BS is equipped with M transmit antennas, the BS can serve the maximum amount of UE for simultaneous transmission in a single time slot. Here, we define S as a maximum number of UE selected for each time slot. However, since the goal of the proposed scheduling technique is secure communication, the BS also needs to manage the leakage to EVEs by beamforming. It is obvious that the BS can sufficiently manage the leakage to EVEs when the number of antennas is much larger than selected UE, i.e., $S \ll M$. Hence, we set the maximum number of selected UE to be much smaller than M.

To select S UE, the selection metric of (5) is performed S times. Then, the set of users that allocated to the t-th time slot can be derived as follows:

$$\mathcal{N}_t = \left\{ n_t^{[1]}, n_t^{[2]}, \cdots, n_t^{[S]} \right\}, \tag{6}$$

where $n_t^{[s]}$ is s-th selected UE at the t-th time slot. As a result, the allocation process of the proposed technique can be summarized as Algorithm 1.

Algorithm 1 Time slot allocation algorithm for user equipment (UE) scheduling.

Input: $\mathbf{h}_{\mathsf{U}}^{[n,t]}, \mathbf{h}_{\mathsf{E}}^{[e,t]} \quad \forall n, \forall e, \forall t$
Output: $\mathcal{N}_t \quad \forall t$
  for $t = 1 : T$ **do**
    $\mathcal{N} = \{1, 2, \cdots, N\}, \quad \mathcal{N}_t = \emptyset$
    for $s = 1 : S$ **do**
      $n_t^{[s]} = \underset{n \in \mathcal{N}}{\operatorname{argmax}} \frac{\left|\mathbf{h}_{\mathsf{U}}^{[n,t]}\right|^2}{\max\limits_{e} \left|\mathbf{h}_{\mathsf{E}}^{[e,t]}\right|^2}$
      $\mathcal{N}_t = \mathcal{N}_t \cup n_t^{[s]}, \quad \mathcal{N} = \mathcal{N} \setminus n_t^{[s]}$
    end for
  end for

After UE scheduling is over for all time slots, the BS designs its transmit beamforming for each time slot based on the CSI of selected UE. Note that the target of the transmit beamforming design of the BS is to maximize the power received at UE while minimizing the power received at EVEs, which means maximizing the secrecy rate. Meanwhile, there is already an ideal solution for designing a beamforming matrix for the maximum secrecy rate wherein both the communication channel and the eavesdropping channel are taken into account [40]. Based on the solution of [40], the BS designs a transmitting beamforming matrix for each time slot for the communication channel of a selected UE and that of EVEs as follows:

$$\mathbf{B}_t = \mathrm{Eig}_S\left(\left(\mathbf{I}_M + \rho \mathbf{H}_{\mathsf{E},t}^H \mathbf{H}_{\mathsf{E},t}\right)^{-1}\left(\mathbf{I}_M + \rho \mathbf{H}_{\mathsf{C},t}^H \mathbf{H}_{\mathsf{C},t}\right)\right), \tag{7}$$

where $\mathbf{H}_{\mathsf{C},t}$ represents a communication channel matrix consisting of S channel vectors of UE that are scheduled for the t-th time slot; i.e., $\mathbf{H}_{\mathsf{C},t} = \left[\mathbf{h}_{\mathsf{C}}^{\left[n_t^{[1]},t\right]T}, \mathbf{h}_{\mathsf{C}}^{\left[n_t^{[2]},t\right]T}, \cdots, \mathbf{h}_{\mathsf{C}}^{\left[n_t^{[S]},t\right]T}\right]^T$. In addition, $\mathbf{H}_{\mathsf{E},t}$ is an eavesdropping channel matrix consisting of channel vectors of EVEs, i.e., $\mathbf{H}_{\mathsf{E},t} = \left[\mathbf{h}_{\mathsf{E}}^{[1,t]T}, \mathbf{h}_{\mathsf{E}}^{[2,t]T}, \cdots, \mathbf{h}_{\mathsf{E}}^{[E,t]T}\right]^T$. The ρ and $\mathbf{I}_M$ indicate transmit signal-to-noise ratio (SNR) and an identity matrix that is $M \times M$ in size, respectively. Moreover, $\mathrm{Eig}_S(\cdot)$ denotes a function for which the output is S eigenvectors that correspond to the highest S eigenvalue.

Furthermore, for the case that multiple pieces of UE are allocated to a single time slot, the inter-user interference needs to be managed. Hence, the BS designs a zero-forcing matrix (a well-known matrix) to eliminate the inter-user interference in a single time slot as follows.

$$\mathbf{Z}_t = \left(\mathbf{H}_{\mathsf{C},t}\mathbf{B}_t\right)^{-1}. \tag{8}$$

As a result, the final beamforming matrix for the t-th time slot in which only one UE is scheduled is $\mathbf{V}_t = \mathbf{B}_t$. By contrast, if $S > 1$, then the final beamforming matrix for the t-th time slot is $\mathbf{V}_t = \mathbf{B}_t\mathbf{Z}_t$, but it is normalized to each of its column vectors that have unit power. It is worth noting that there is no additional signaling process in the overall procedure of the proposed RCR technique except channel estimation. Since the RCR technique does not require information exchange between BS and RIS, it can be easily implemented to practical communication systems. Briefly, the transmit beamforming matrix design of BS can be described as Algorithm 2.

Algorithm 2 Transmit beamforming design at the base station (BS) for all time slots.

Input: $S, \mathbf{h}_{\mathsf{U}}^{[n,t]}, \mathbf{h}_{\mathsf{E}}^{[e,t]}, \mathcal{N}_t \quad \forall n, \forall e, \forall t$
Output: $\mathbf{V}_t \quad \forall t$
  for $t = 1 : T$ **do**
    $\mathbf{H}_{\mathsf{C},t} = \left[\mathbf{h}_{\mathsf{C}}^{\left[n_t^{[1]},t\right]T}, \mathbf{h}_{\mathsf{C}}^{\left[n_t^{[2]},t\right]T}, \cdots, \mathbf{h}_{\mathsf{C}}^{\left[n_t^{[S]},t\right]T}\right]^T$
    $\mathbf{H}_{\mathsf{E},t} = \left[\mathbf{h}_{\mathsf{E}}^{[1,t]T}, \mathbf{h}_{\mathsf{E}}^{[2,t]T}, \cdots, \mathbf{h}_{\mathsf{E}}^{[E,t]T}\right]^T$
    $\mathbf{B}_t = \mathrm{Eig}_S\left(\left(\mathbf{I}_M + \rho \mathbf{H}_{\mathsf{E},t}^H \mathbf{H}_{\mathsf{E},t}\right)^{-1}\left(\mathbf{I}_M + \rho \mathbf{H}_{\mathsf{C},t}^H \mathbf{H}_{\mathsf{C},t}\right)\right)$
    if $S > 1$ **then**
      $\mathbf{Z}_t = \left(\mathbf{H}_{\mathsf{C},t}\mathbf{B}_t\right)^{-1}$
      $\mathbf{V}_t = \mathbf{B}_t\mathbf{Z}_t$
    else
      $\mathbf{V}_t = \mathbf{B}_t$
    end if
    All column vectors of $\mathbf{V}_t$ are normalized to the unit norm.
  end for

After beamforming design is over, the DTD starts. Note that DTD consists of βT time slots as described in the beginning of this chapter. Moreover, in DTD, all RISs repeat the same reflection matrices β times. As a result, it is obvious that all UE and EVEs will use exactly the same communication channel in the DTD as in the PSD β. Therefore, the BS can utilize the designed beamforming matrices, $\mathbf{V}_t$, in DTD, since the same channels as for PSD will be repeated in DTD. Then, the signal received at the n-th UE and the e-th EVE in the t-th time slot can be derived as follows.

$$\begin{aligned} y_{n,t} &= \mathbf{h}_{\mathsf{U}}^{[n,t]}\mathbf{V}_t x_{n,t} + z_{n,t}, \\ y_{e,t} &= \mathbf{h}_{\mathsf{E}}^{[e,t]}\mathbf{V}_t x_{n,t} + z_{e,t}, \end{aligned} \tag{9}$$

respectively, where $x_{n,t}$ is the original signal of n-th UE at the t-th time slot. In addition, $z_{n,t}$ and $z_{e,t}$ are the additive Gaussian noise of n-th UE and e-th EVEs in the t-th time slot, which follows either a zero mean or a unit variance Gaussian distribution, i.e., $\mathcal{CN}(0,1)$, respectively.

Finally, the secrecy rate performance of the proposed RCR technique can be calculated as follows.

$$\mathsf{SR} = \frac{1}{T}\sum_{t=1}^{T}\sum_{s=1}^{S}\left[\log_2\left(1 + \rho\left|\mathbf{h}_{\mathsf{U}}^{\left[n_t^{[s]},t\right]}\mathbf{v}_t^{[s]}\right|^2\right) - \log_2\left(1 + \rho \max_e \left|\mathbf{h}_{\mathsf{E}}^{[e,t_n]}\mathbf{v}_t^{[s]}\right|^2\right)\right], \tag{10}$$

where $\mathbf{V}_t = \left[\mathbf{v}_t^{[1]}, \mathbf{v}_t^{[2]}, \cdots, \mathbf{v}_t^{[S]}\right]$. Here, the physical meaning of the secrecy rate is the maximum data rate that can be securely delivered to legitimate users without leakage to eavesdroppers.

4. Numerical Results

In this section, we validate the performance of proposed RCR technique in terms of secrecy rate. For the simulation, we used Matlab 2019a software and Monte Carlo simulation method by realizing random channel for each iteration. Moreover, we set the two reference technique which are non-RIS case and random scheduling for the comparison with proposed RCR technique. Non-RIS case is that only direct LOS channel between BS and UE or EVE is available, since there is no RIS in the network. Hence, only optimal beamforming design of BS is utilized for PLS enhancement. In addition, random scheduling

is that UE are randomly scheduled at time slot. Note that also in random scheduling, BS designs optimal transmit beamforming as [40].

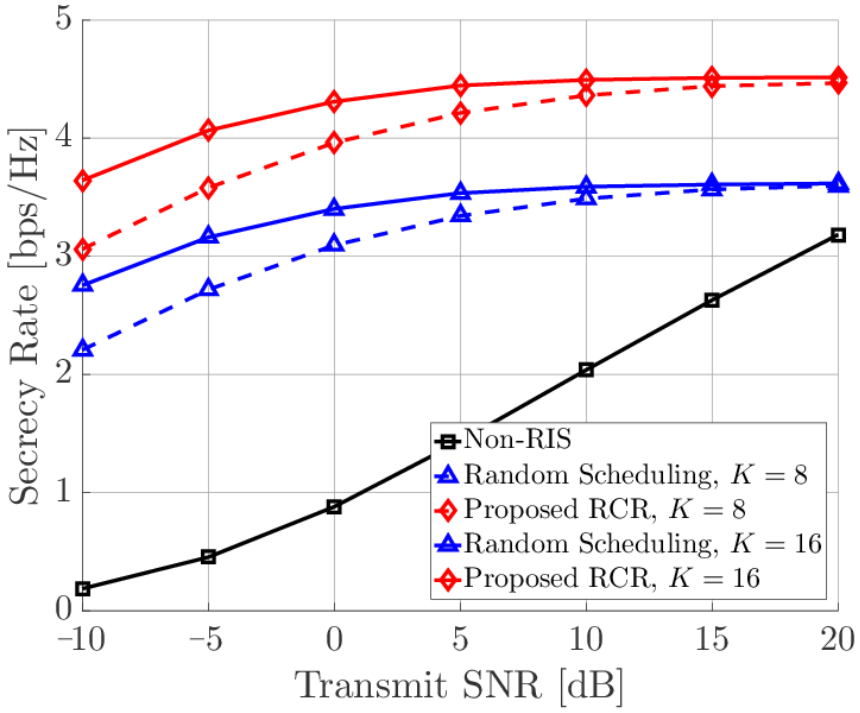


Figure 3. Secrecy rate performance according to transmitted SNR.

In Figure 3, the secrecy rate performance of proposed RCR technique is compared with reference techniques according to the transmit SNR (ρ), where $M = 4$, $L = 16$, $S = 1$, $N = 10$, $T = 10$, and $E = 4$. It is shown that performance of proposed RCR technique and that of random scheduling were saturated as transmit SNR increased. However, even the performance of the proposed RCR technique was saturated as SNR increases; it outperformed all other reference techniques; even the non-RIS case showed significant enhancement as SNR increases. Furthermore, it is shown that as the number of RISs increases, the performance of proposed RCR technique can achieve be saturated more quickly.

The secrecy rate performance of proposed RCR technique according to the number of UE (N) is shown in Figure 4, where $M = 4$, $L = 16$, $S = 1$, $K = 16$, $T = 10$, and $E = 4$. Since pieces of UE are randomly scheduled in the non-RIS case and random scheduling, it is shown that their performance is not enhanced even as the number of pieces of UE increases. However, proposed RCR technique allocates the best UE for the time slot; hence, it can achieve scheduling gain from a large amount of UE. Therefore, proposed RCR technique achieved the highest performance according to number of UE.

Figure 5 shows the secrecy rate performances of all techniques according to the number of RISs (K), where $M = 4$, $L = 16$, $S = 1$, $T = 10$, $N = 10$, and $\rho = 10$ dB. It is shown that proposed RCR technique also outperformed other reference techniques according to the number of RISs; see Figures 3 and 4. Obviously, the non-RIS case is not effected by the number of RISs because it is based on the environment in which RISs do not exist.

Most importantly, the performances of the RIS-based techniques (proposed and random scheduling) do not increase linearly as the number of RISs increases, but they do get saturated. As a result, it is shown that there is no need to deploy many RISs in the network for the proposed RCR technique.

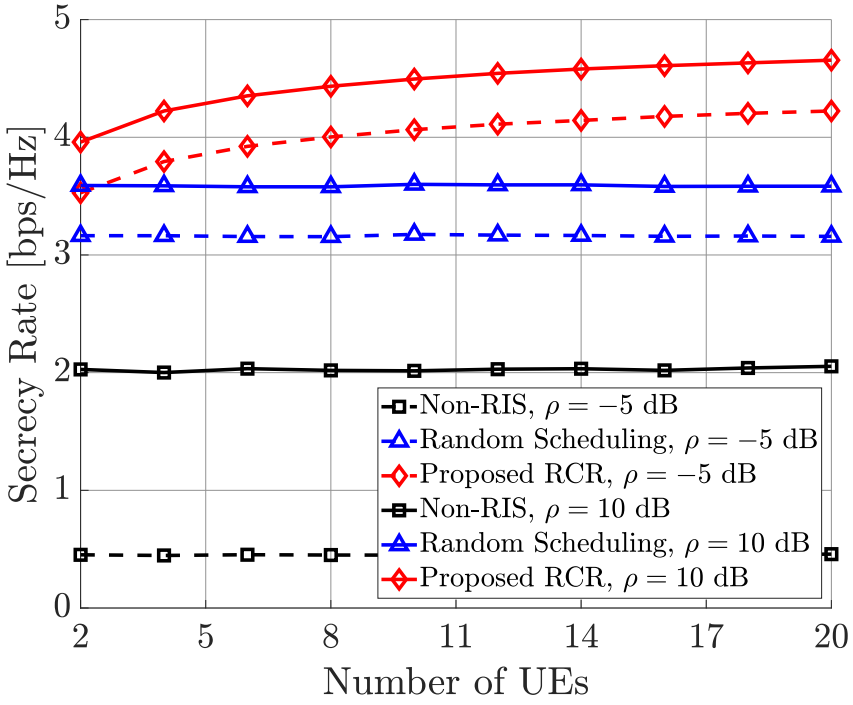


Figure 4. Secrecy rate performance according to number of UE.

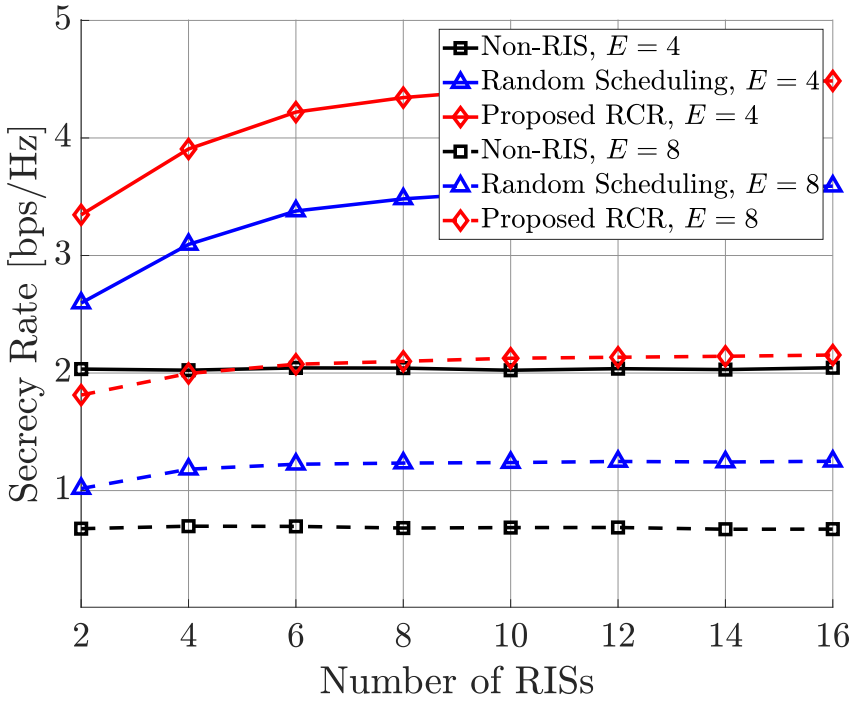


Figure 5. Secrecy rate performance according to number of RISs.

5. Conclusions

In this paper, we proposed a reconfigurable intelligent surface (RIS)-based channel randomization (RCR) technique for improving physical-layer security (PLS) for a time-division duplex (TDD) downlink cellular wire-tap network consisting of a single base station (BS) with multiple antennas, multiple legitimate pieces of user equipment (UE), multiple potential eavesdroppers (EVEs), and multiple RISs with multiple passive elements. In the proposed technique, each RIS pseudo-randomly generates multiple reflection matrices and utilizes pilot signal duration (PSD) in uplink and data transmission duration (DTD) in

downlink for user scheduling. As a result, exactly same communication channel for the PSD will be used for the DTD so that BS can schedule the UE with information of PSD without uncertainty. In addition, the UE are scheduled to achieve the highest secrecy rate and the transmit beamforming of BS is also designed to achieve best secrecy rate for UE scheduled in a certain time slot. Through computer simulations, we validated that the proposed RCR technique achieves higher secrecy rate performance than the conventional techniques.

Author Contributions: Formal analysis, J.Y.; Investigation, W.S., J.Y., and B.C.J.; methodology, J.Y.; project administration, B.C.J.; resources, B.C.J.; software, J.Y.; Supervision, B.C.J.; validation, W.S. writing—original draft, W.S. and J.Y.; and writing—review and editing, B.C.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: This work has been supported by the Future Combat System Network Technology Research Center program of Defense Acquisition Program Administration and Agency for Defense Development. (UD190033ED).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AN	Artificial-noise
AP	Access point
BS	Base station
CSI	Channel state information
DTD	Data transmission duration
EVE	Eavesdropper
IoT	Internet-of-things
IRS	Intelligent reflecting surface
LOS	Line-of-sight
MISO	Multiple-input multiple-output
mmWave	Millimeter wave
NOMA	Non-orthogonal multiple access
PLS	Physical-layer security
PSD	Pilot signal duration
RCR	RIS-based Channel Randomization
RIS	Reconfigurable intelligent surface
SIMO	Single-input multiple-output
SINR	Signal to interference-plus-noise ratio
SNR	Signal-to-noise ratio
TDD	Time-division duplex
THz	Tera-hertz
UE	User equipment
ULA	Uniform linear array

References

1. Cui, T.J.; Qi, M.Q.; Wan. X.; Zhao, J.; Cheng, Q. Coding metamaterials, digital metamaterials and programmable metamaterials. *Light. Sci. Appl.* **2014**, *3*, e218. [CrossRef]
2. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Veh. Tech. Mag.* **2019**, *14*, 28–41. [CrossRef]
3. Wu, Q.; Zhang, R. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless networks. *IEEE Commun. Mag.* **2020**, *58*, 106–112. [CrossRef]
4. Huang, C.; Hu, S.; Alexandropoulos, G.C.; Zappone, A.; Yuen, C.; Zhang, R.; Renze, M.D.; Debbah, M. Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [CrossRef]

5. Basar, E.; Renzo, M.D.; Rosny, J.D.; Debbah, M.; Alouini, M.-S.; Zhang, R. Wireless communications through reconfigurable intelligent surfaces. *IEEE Access* **2019**, *7*, 116753–116773. [CrossRef]
6. Wu, Q.; Zhang, R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5394–5409. [CrossRef]
7. ElMossallamy, M.A.; Zhang, H.; Sultan, R.; Seddik, K.G.; Song, L.; Li, G.Y.; Han, Z. On spatial multiplexing using reconfigurable intelligent surfaces. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 226–230. [CrossRef]
8. Chu, Z.; Xiao, P.; Shojafar, M.; Mi, D.; Mao, J.; Hao, W. Intelligent reflecting surface assisted mobile edge computing for internet of things. *IEEE Wirel. Commun. Lett.* **2020**. [CrossRef]
9. Özdogan, Ö.; Björnson, E.; Larsson, E.G. Using intelligent reflecting surfaces for rank improvement in MIMO communications. In Proceedings of the 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020.
10. Shiu, Y.-S.; Chang, S.Y.; Wu, H.-C.; Huang, S.C.-H.; Chen, H.-H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
11. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.-K.; Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
12. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
13. Li, Z.; Guan, L.; Li, C.; Radwan, A. A secure intelligent spectrum control strategy for future THz mobile heterogeneous networks. *IEEE Commun. Mag.* **2018**, *56*, 116–123. [CrossRef]
14. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surv. Tuts.* **2020**, *22*, 196–248. [CrossRef]
15. Jin, H.; Shin, W.-Y.; Jung, B.C. On the multi-user diversity with secrecy in uplink wiretap networks. *IEEE Commun. Lett.* **2013**, *17*, 1778–1781. [CrossRef]
16. Chorti, A.; Perlaza, S.M.; Han, Z.; Poor, H.V. On the resilience of wireless multiuser networks to passive and active eavesdroppers. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1850–1863. [CrossRef]
17. Kapetanovic, D.; Zheng, G.; Rusek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* **2015**, *53*, 21–27. [CrossRef]
18. Joung, J.; Choi, J.; Jung, B.C.; Yu, S. Artificial noise injection and its power loading methods for secure space-time line coded systems. *Entropy* **2019**, *21*, 515. [CrossRef]
19. Choi, J.; Joung, J.; Jung, B.C. Space-time line code for enhancing physical layer security of multiuser MIMO uplink transmission. *IEEE Syst. J.* **2020**. [CrossRef]
20. Son, W.; Jang, H.; Jung, B.C. A Pseudo-random beamforming technique for improving physical-layer security of MIMO cellular networks. *Entropy* **2019**, *21*, 1038. [CrossRef]
21. Abbas, M.A.; Song, H.; Hong, J.-P. Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 969–980. [CrossRef]
22. Bang, I.; Jung, B.C. Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers. *IEEE Access* **2019**, *7*, 127078–127089. [CrossRef]
23. Son, W.; Nam, H.; Shin, W.-Y.; Jung, B.C. Secrecy outage analysis of multiuser downlink wiretap networks with potential eavesdroppers. *IEEE Syst. J.* **2020**. [CrossRef]
24. Lu, X.; Hossain, E.; Shafique, T.; Feng, S.; Jiang, H.; Niyato, D. Intelligent reflecting surface enabled covert communications in wireless networks. *IEEE Netw.* **2020**, *34*, 148–155. [CrossRef]
25. Almohamad, A.; Tahir, A.M.; Al-Kababji, A.; Furqan, H.M.; Khattab, T.; Hasna, M.O.; Arslan, H. Smart and secure wireless communications via reflecting intelligent surfaces: A short survey. *IEEE Open J. Commun. Soc.* **2020**, *1*, 1442–1456. [CrossRef]
26. Yu, X.; Xu, D.; Schober, R. Enabling secure wireless communications via intelligent reflecting surfaces. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019.
27. Cui, M.; Zhang, G.; Zhang, R. Secure wireless communication via intelligent reflecting surface. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1410–1414. [CrossRef]
28. Chu, Z.; Hao, W.; Xiao, P.; Shi, J. Intelligent reflecting surface aided multi-antenna secure transmission. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 108–112. [CrossRef]
29. Xiu, Y.; Zhang, Z. Secure wireless transmission for intelligent reflecting surface-aided millimeter-wave systems. *IEEE Access* **2020**, *8*, 192924–192935. [CrossRef]
30. Qiao, J.; Alouini, M.-S. Secure transmission for intelligent reflecting surface-assisted mmWave and Terahertz systems. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1743–1747. [CrossRef]
31. Chen, J.; Liang, Y.-C.; Pei, Y.; Guo, H. Intelligent reflecting surface: A programmable wireless environment for physical layer security. *IEEE Access* **2019**, *7*, 82599–82612. [CrossRef]
32. Lu, X.; Yang, W.; Guan, X.; Wu, Q.; Cai, Y. Robust and secure beamforming for intelligent reflecting surface aided mmWave MISO systems. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 2068–2072. [CrossRef]
33. Xu, D.; Yu, X.; Sun, Y.; Ng, D. W.K.; Schober, R. Resource allocation for secure IRS-assisted multiuser MISO systems. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019.

34. Guan, X.; Wu, Q.; Zhang, R. Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?. *IEEE Wirel. Commuin. Lett.* **2020**, *9*, 778–782. [CrossRef]
35. Wang, H.-M.; Bai, J.; Dong, L. Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI. *IEEE Signal Process. Lett.* **2020**, *27*, 1300–1304. [CrossRef]
36. Yu. X.; Xu, D.; Sun, Y.; Ng, D.W.K.; Schober, R. Robust and secure wireless communications via intelligent reflecting surfaces. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2637–2652. [CrossRef]
37. Hong, S.; Pan, C.; Ren, H.; Wang, K.; Nallanathan, A. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. *IEEE Trans. Commun.* **2020**, *68*, 7851–7866. [CrossRef]
38. Hong, S.; Pan, C.; Ren, H.; Wang, K.; Chai, K.K.; Nallanathan, A. Robust transmission design for intelligent reflecting surface aided secure communication systems with imperfect cascaded CSI. *IEEE Trans. Wirel. Commun.* **2020**. [CrossRef]
39. Chu, Z.; Hao, W.; Xiao, P.; Mi, D.; Liu, Z.; Khalily, M.; Kelly, J.R.; Feresidis, A.P. Secrecy rate optimization for intelligent reflecting surface assisted MIMO system. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1655–1669. [CrossRef]
40. Khisti, A.; Wornell, G.W. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 3088–3104. [CrossRef]