EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

STAR-RIS-assisted key generation method in quasi-static environment

Yang Ma[1], Liquan Chen[1,2*], Tianyu Lu[1], Yufan Song[1] and Kailin Cao[1]

*Correspondence:
lqchen@seu.edu.cn

[1] School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China
[2] Purple Mountain Laboratory, Nanjing 210096, China

Abstract

In this paper, we introduce a new method to solve the low-entropy problem in a quasi-static environment. We utilize a simultaneous transmission and reflection reconfigurable intelligent surface (STAR-RIS) that transmits and reflects incoming signals to users located on different sides of the surface. Specifically, we design the flow of multi-user channel probing when STAR-RIS is assisted, analyze and derive the analytical expression of the secret key capacity (SKC) of STAR-RIS-assisted system from the perspective of information theory, and finally analyze how to maximize the SKC and sum of all users under three different working protocols of STAR-RIS. The simulation results show that: (1) STAR-RIS can achieve better SKC performance than the conventional reflection/transmission RIS; and (2) the SKC is determined by the number of STAR-RIS elements, correlation coefficient, pilot length and RIS-reflected channel quality, and the time switching protocol can obtain higher SKC than the energy splitting protocol and mode switching protocol.

Keywords: Physical layer key generation, Reconfigurable intelligent surface, Key capacity, Wireless secure communication

1 Introduction

Physical layer key generation can achieve information-theoretical security by using the characteristics of the wireless channel, such as reciprocity and randomness of the wireless channel [1] [2]. A legitimate user can safely generate a pair of shared keys after four main steps: channel probing, quantization, information reconciliation and privacy amplification [3]. Currently, the foundational theory of physical layer key generation has achieved a relatively comprehensive status. However, practical implementation faces certain challenges, particularly in terms of security and performance constraints imposed by the natural environment [4]. In other words, key generation performance depends on the channel fluctuations caused by the movement of the surrounding environment.

However, in quasi-static environments, the key generation rate (KGR) is greatly limited due to the low entropy that can be extracted from the channel [5]. To overcome the constraints of the natural environment, reconfigurable intelligent surface (RIS) is usually used in quasi-static environments to assist communication [6]. RIS can manipulate electromagnetic waves through its numerous reflecting elements [7]. When the signal is illuminated on the reflecting elements, the elements can efficiently modify the amplitude,

© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

phase and frequency of electromagnetic waves, thus realizing the real-time reconfiguration of the electromagnetic environment and the dynamic programming of the wireless channel [8]. Since RIS can be viewed as a passively reflected planar array, this intelligent reconstruction of the electromagnetic space by RIS does not consume additional energy [9]. The low hardware cost and energy consumption of RIS makes it an ideal assistant in the formation of fluctuating channels between legitimate users, therefore providing artificial randomness for the generation of keys. Jin et al. minimized transmit power while guaranteeing KGR [10]. Jiao et al. proposed a reconfiguration strategy to improve the KGR in slow-fading scenarios [11]. Yang maximized the achievable rate by jointly optimizing the transmit power allocation and the RIS passive array reflection coefficients [12]. Tan et al. studied joint optimization about beam-forming, RIS phase shift and energy harvesting of IoT devices for maximizing EE of the multiple-input single-input downlink system with multiple IoT devices and an energy harvesting device [13]. Lu et al. obtained performance improvement through the joint design of precoding and phase shift matrix [14]. Ji et al. explored the lower limit of secret key capacity (SKC) for RIS-assisted physical layer key generation when there are multiple non-collusion eavesdroppers, and the derived analytical expression accurately describes the influence of channel correlation among legitimate users, eavesdroppers and RIS on key capacity [15]. In Ref. [16], a four-step channel probing protocol was designed for RIS-assisted key generation by utilizing the randomness of direct and reflected channels, and lower and upper bounds of key capacity expressions were derived in the presence of eavesdrops. Li et al. derived the expression of key capacity and optimizes the configuration of RIS to maximize the total key capacity on independent fading channels and related fading channels in the presence of multiple users [17].

Although RIS-assisted physical layer key generation technology has made a great success, RIS can only reflect or transmit the incident signal, which reduces the flexibility of the system [18]. In order to obtain the channel environment for each device in the system after RIS reconstruction in channel probing, it is necessary for all devices to be located on the same side of RIS, or to extend the coverage by deploying multiple RIS [19]. Xiao investigated the physical layer security (PLS) of a simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS)-aided rate-splitting multiple access (RSMA) systems in the presence of an eavesdropper [20]. Liu put forward the simultaneous transmission and reflection reconfigurable intelligent surface (STAR-RIS) which can not only reflect the incident signal but also transmit the incident signal to the other side through the new RIS, thereby improving the coverage of the RIS to create a controllable channel environment [21]. This innovative approach is further supported by the findings presented in Ref. [22], which proves that STAR-RIS elements with scalar surface impedance exhibit the same transfer and reflection coefficients on both sides, demonstrating reciprocity similar to traditional RIS. However, at present, the relevant analysis and solution of STAR-RIS in physical layer key generation have not been studied, so we will focus on the feasibility, technical ideas, implementation ways and implementation effects of STAR-RIS in assisting the physical layer key generation.

In this paper, we derive the key capacity expressions of STAR-RIS under three different protocols and analyze the optimization model for key capacity within the system. STAR-RIS-assisted solutions aim to maximize the key capacity of the system by addressing the diverse needs of different users. Through simulation tests, we demonstrate that STAR-RIS can provide more powerful, rich and fine-grained auxiliary capabilities for physical layer key generation.

Symbols: Lowercase letters, bold lowercase letters and bold uppercase letters represent scalars, vectors and matrices, respectively. $\mathcal{CN}\left(\mu,\sigma^2\right)$represents the circularly symmetric complex Gaussian distribution (CSCG) with mean μ and standard deviation σ. $(\cdot)^{-1}$, $\bar{(\cdot)}$, $(\cdot)^T$ and $(\cdot)^H$ represent the inverse transformation, conjugate, transpose and conjugate transpose operations, respectively.

2 Methods

In this section, we first propose our system model. Meanwhile, we analyze the upper and lower bounds of the key capacity and propose an optimization scheme.

2.1 STAR-RIS-assisted system model

In this section, the system model is presented by considering the STAR-RIS-assisted key generation under the attack of multiple eavesdroppers.

As shown in Fig. 1, a STAR-RIS-assisted multi-user key generation system is constructed in this chapter, which consists of a wireless base station (Alice), a STAR-RIS, K user terminals (UT)s and K eavesdroppers (Eves). All participants, including Alice, UTs and Eves, are equipped with a single antenna, p legal user UTs are located in the reflection space of STAR-RIS, q legal user UTs are located in the transmission space of STAR-RIS, and $K=p+q$. Alice's task is to generate the key $\kappa=\{\kappa_1,\kappa_2,\cdots,\kappa_K\}$ based on the wireless channel between the base station and UTs. The multi-user key generation in this chapter is different from the group key generation because the key generated between Alice and each UT is not the same.

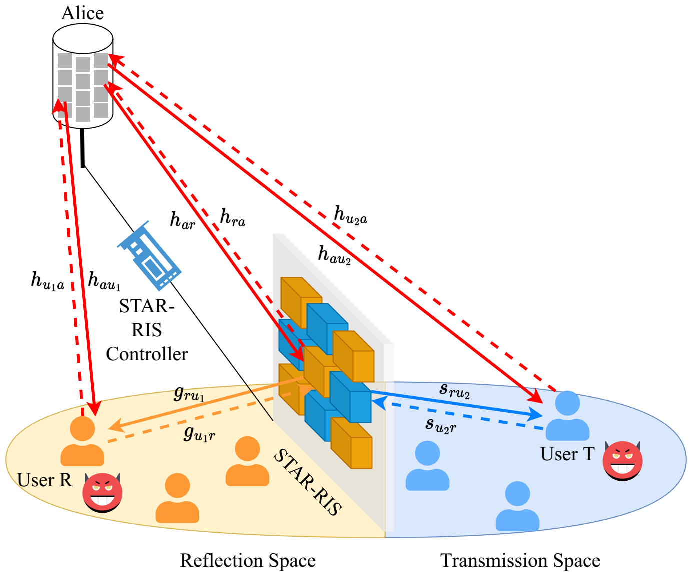


Fig. 1 STAR-RIS-assisted key generation system model

The communication between Alice and UTs is based on time-division duplex (TDD) mode, and Ref. [22] states that when the surface element impedance of STAR-RIS can be characterized by scalars, STAR-RIS can exert the same effect on signals incident from different surfaces (that is, upstream and downstream), thus ensuring the reciprocity of upstream and downstream cascaded channels in a single-channel probing. As shown in Fig. 2, signals x_a and x_b are incoming signals from space A and space B, respectively; $T_m^{A,B}$ and $T_m^{B,A}$ are the transmission coefficients of the mth element when the signal enters space B from space A and space A from space B; and R_m^A and R_m^B are the reflection coefficients of the mth element on side A and side B of space, respectively. In this case, $T_m^{A,B} = T_m^{B,A}$ and $R_m^A = R_m^B$.

The Eves do not initiate active attacks, and Eves do not exchange information with each other. Each eavesdropper Eve eavesdrops on the keys in the collective κ based on her own observations of the channel information and all the information exchanged over the common channel. In addition, UTs in the system are treated as curious users, but each UT does not intend to eavesdrop on other users' keys, and they do not collude with other UTs or Eves.

In Fig. 1, STAR-RIS operates under mode switching (MS) protocol, and the reflection coefficient matrix and transmission coefficient matrix of STAR-RIS can be expressed as

$$\Theta_r^{\mathrm{MS}} = \mathrm{diag}\left(\sqrt{\beta_1^r}e^{j\theta_1^r}, \sqrt{\beta_2^r}e^{j\theta_2^r}, \ldots, \sqrt{\beta_M^r}e^{j\theta_M^r}\right) \tag{1}$$

and

$$\Theta_t^{\mathrm{MS}} = \mathrm{diag}\left(\sqrt{\beta_1^t}e^{j\theta_1^t}, \sqrt{\beta_2^t}e^{j\theta_2^t}, \ldots, \sqrt{\beta_M^t}e^{j\theta_M^t}\right) \tag{2}$$

where $\beta_m^r, \beta_m^t \in \{0,1\}$, $\beta_m^r + \beta_m^t = 1$ and $\theta_m^r, \theta_m^t \in [0, 2\pi)$, $\forall m \in M$. The mode switching protocol divides the elements to reflect and transmit signals. In the optimization scheme, we also consider the other two operating protocols of STAR-RIS, that is, energy splitting protocol and time switching protocol, as shown in Fig. 3.

During the downlink channel probing, Alice broadcasts the pilot signal x_{dl}, while in the upstream channel probing, user UTs simultaneously send the pilot signal $x_{ul,k} \in \mathcal{C}^{1\times K}, k \in \{1, 2, \cdots, K\}$ to Alice. For Alice to distinguish each user, each user's pilot signal satisfies the orthogonal condition:

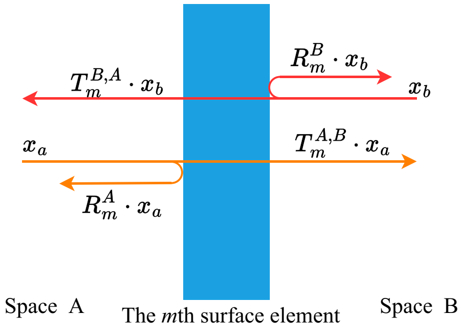
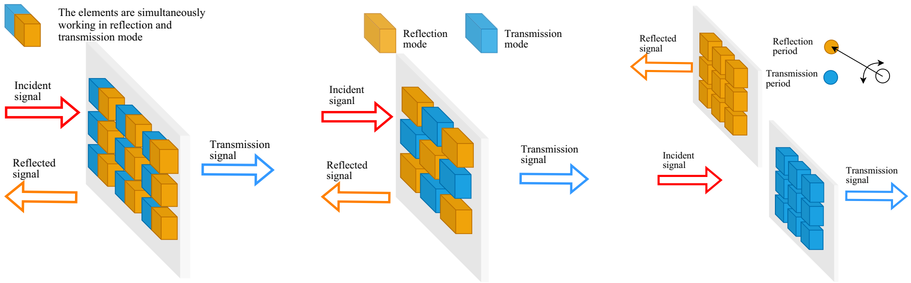


Fig. 2 Model when the signal is incident from both sides of the STAR-RIS



(a) Energy Segmentation (ES) (b) ModeSwitching (MS) (c) Time Switching (TS)

Fig. 3 Three working protocols of STAR-RIS

$$x_{ul,k}\left(x_{ul,k'}\right)^{H} = \begin{cases} 1, \; k = k' \\ 0, \; k \neq k' \end{cases}. \tag{3}$$

The signals received by users k and Alice can be expressed as

$$y_k^{dl} = \left(h_{ak} + \sum_{m=1}^{M} h_{rk}^m \sqrt{\beta_m} e^{j\theta_m} h_{ar}^m\right) x_{dl} + n'_{dl,k}, \tag{4}$$

$$y_{ul} = \sum_{k=1}^{K} \left(h_{ka} + \sum_{m=1}^{M} h_{ra}^m \sqrt{\beta_m} e^{j\theta_m} h_{kr}^m\right) x_{ul,k} + n_{ul}, \tag{5}$$

where $n'_{dl,k}$ is the additive white Gaussian noise, whose mean value is 0 and variance is σ^2; $h_{rk} = g_{rk}$ if the user k is in the reflection region and $h_{rk} = s_{rk}$ if the user k is in the transport region. h_{ak} is a direct channel between Alice and the user k; $h_{ar} \in \mathcal{C}^{(M\times 1)}$ is a channel between Alice and STAR-RIS; $g_{rk} \in \mathcal{C}^{(M\times 1)}$ is a channel between STAR-RIS and the user k in the reflection area; and $s_{rk} \in \mathcal{C}^{(M\times 1)}$ is a channel between STAR-RIS and the user k in the transmission area. We consider a narrow-band quasi-static block-fading channel. Within a block, h_{ak}, h_{ar}, g_{rk} and s_{rk} do not change. The system obtains randomness by changing the phase shift matrix.

Then, the user k and Alice estimate the combined channel by least-squares method:

$$h_k^{dl} = y_k^{dl} x_{dl}^{*} = h_{ak} + \sum_{m=1}^{M} h_{rk}^m \sqrt{\beta_m} e^{j\theta_m} h_{ar}^m + n_{dl,k}, \tag{6}$$

$$h_k^{ul} = h_{ka} + \sum_{m=1}^{M} h_{ra}^m \sqrt{\beta_m} e^{j\theta_m} h_{kr}^m + n_{ul,k}. \tag{7}$$

The link between Alice-STAR-RIS-UT can be defined as $r_{uv} = \left[r_{uv}^1, \ldots, r_{uv}^M\right]$, where $\{u, v\} = \{a, k\}$. Specifically, if the user k is in the reflection region, then $r_{uv}^m = g_{rk}^m h_{ur}^m$, where r_{uv}^m stands for mth sub-reflection channel. If the user k is in the transport zone, then $r_{uv}^m = s_{rk}^m h_{ur}^m$, where r_{uv}^m represents the mth sub-transport channel. Therefore, the downward CSI derived from formula (4) can be rewritten as

$$h_k^{dl} = h_{ak} + \Theta^{MS} r_{ak}^T + n_{dl,k}. \tag{8}$$

Similarly, the ascending CSI derived from formula (5) can be rewritten as

$$h_k^{ul} = h_{ka} + \Theta^{MS} r_{ka}^T + n_{ul,k}. \tag{9}$$

After Q rounds of pilot exchange between Alice and UTs, the acquired combined channel vector can be expressed as

$$\widetilde{h}_D = \left[\widetilde{h}_D(1), \widetilde{h}_D(2), \cdots, \widetilde{h}_D(Q)\right], D \in \{A, k, E\}. \tag{10}$$

2.2 Secret key capacity and system optimization

The secret key capacity can be defined as the maximum achievable rate at which Alice and a single user can successfully establish a key through a sufficient number of channel probes while ensuring that the information obtained by Eve remains sufficiently limited and secure [23]. When the distance between Eve and Alice and a user exceeds half wavelength [24], Eve cannot obtain information about the legitimate channel from its detection value of the legitimate channel, and the secret key capacity at this time is the mutual information of the channel sampling value between Alice and the user $I\left(\widetilde{h}_A; \widetilde{h}_k\right)$. When Eve is less than half a wavelength away from a user, Eve may obtain information about the legitimate channel from its detection value of the legitimate channel. In Ref. [25], the secret key capacity is defined as an interval value with upper and lower bounds:

$$C_{sk} \geq I\left(\widetilde{\mathbf{h}}_A; \widetilde{\mathbf{h}}_k\right) - \min\left[I\left(\widetilde{\mathbf{h}}_A; \widetilde{\mathbf{h}}_E\right), I\left(\widetilde{\mathbf{h}}_k; \widetilde{\mathbf{h}}_E\right)\right], \tag{11}$$

$$C_{sk} \leq \min\left[\mathrm{I}\left(\widetilde{\mathbf{h}}_\mathrm{A}; \widetilde{\mathbf{h}}_\mathrm{k}\right), \mathrm{I}\left(\widetilde{\mathbf{h}}_\mathrm{A}; \widetilde{\mathbf{h}}_\mathrm{k} \middle| \widetilde{\mathbf{h}}_\mathrm{E}\right)\right]. \tag{12}$$

Take Alice as an example, the channel measurement h_k^{ul} follows the distribution $h_k^{ul} \sim \mathcal{CN}\left(0, \sigma^2_{h_k^{ul}}\right)$, where $\sigma^2_{h_k^{ul}}$ can be expressed as $\sigma^2_{h_k^{ul}} = \sigma^2_{h_{ka}} + \sum_{m=1}^{M} \beta_m \sigma^2_{r_{ka}^m}$. Because the channels are reciprocal in coherence time, that is, $h_{ak} = h_{ka}, r_{ak}^m = r_{ka}^m, m = 1, ..., M$. Therefore, it can be obtained that $\sigma^2_{h_k^{dl}} = \sigma^2_{h_k^{ul}}$, so the channel estimation variance of legitimate users is expressed as $\sigma^2_{h_{au}}$, that is, $\sigma^2_{h_k^{dl}} = \sigma^2_{h_k^{ul}} = \sigma^2_{h_{au}}$. Since noise is usually independent and uniformly distributed, the estimated noise variance for each user is set to σ_z^2. Therefore, the mutual information between Alice and the user can be expressed as

$$I\left(h_k^{dl}; h_k^{ul}\right) = \log_2\left(1 + \frac{\left(\sigma^2_{h_{ak}} + \sum_{m=1}^{M} \beta_m \sigma^2_{r_{ak}^m}\right)^2 / \sigma_z^4}{1 + 2\left(\sigma^2_{h_{ak}} + \sum_{m=1}^{M} \beta_m \sigma^2_{r_{ak}^m}\right) / \sigma_z^2}\right). \tag{13}$$

When each Eve is located less than half a wavelength away from base station Alice or user UT, the lower bound of the secret key capacity can be expressed as

$$C_{LB} \geq \log_2\left(1 + \frac{\sigma_{h_{au}}^4/\sigma_z^4}{1 + 2\sigma_{h_{au}}^2/\sigma_z^2}\right) - \log_2\left(1 + \frac{|\rho|^2\sigma_{h_{au}}^4/\sigma_z^4}{1 + \left(1 - |\rho|^2\right)\sigma_{h_{au}}^4/\sigma_z^4 + 2\sigma_{h_{au}}^2/\sigma_z^2}\right), \tag{14}$$

The upper bound of the secret key capacity can be expressed as

$$C_{UB} \leq \log_2\left(\frac{\left[\left(1 - |\rho|^2\right)\sigma_{h_{au}}^4/\sigma_z^4 + 2\sigma_{h_{au}}^2/\sigma_z^2 + 1\right]^2}{\left(1 + \sigma_{h_{au}}^2/\sigma_z^2\right)\left[2\left(1 - |\rho|^2\right)\sigma_{h_{au}}^4/\sigma_z^4 + 3\sigma_{h_{au}}^2/\sigma_z^2 + 1\right]}\right) \tag{15}$$

As shown in the analytical expression of the secret key capacity, it is affected by the correlation coefficients between the legitimate and eavesdropping channels, the channel quality and the estimation noise.

3 Secret key capacity optimization under different protocols

In this section, the secret key capacity is analyzed under mode switching (MS), time switching (TS) and energy switching (ES) protocols. Besides, three optimization problems are formulated to improve the secret key rate of the STAR-RIS-assisted system.

3.1 Secret key capacity optimization under MS protocol

In the MS protocol that operates STAR-RIS, in addition to the reflection and transmission coefficient matrix as expressed in Sect. 2, the reflection and transmission coefficient matrix under the MS protocol can also be expressed as

$$\Theta_r^{\mathrm{MS}} = \mathrm{diag}\left(e^{j\theta_1^r}, e^{j\theta_2^r}, \ldots, e^{j\theta_{M_r}^r}\right) \tag{16}$$

and

$$\Theta_t^{\mathrm{MS}} = \mathrm{diag}\left(e^{j\theta_{M_r+1}^t}, e^{j\theta_{M_r+2}^t}, \ldots, e^{j\theta_M^t}\right) \tag{17}$$

In this representation, the reflection coefficient matrix contains only M_r elements that work in the reflection mode, and these elements are numbered with $1, 2, \ldots, M_r$; the transmission coefficient matrix contains only $M - M_r = M_t$ elements working in the transmission mode, and these elements are numbered with $M_r + 1, M_r + 2, \ldots, M$. Therefore, when the eavesdropping channel is not related to the legitimate channel, the secret key capacity of Alice and the user in the reflected region can be expressed as

$$I_r\left(h_k^{dl}; h_k^{ul}\right) = \log_2\left(1 + \frac{\left(\sigma_{h_{ak}}^2 + \sum_{m=1}^{M_r}\sigma_{r_{ak}^m}^2\right)^2/\sigma_z^4}{1 + 2\left(\sigma_{h_{ak}}^2 + \sum_{m=1}^{M_r}\sigma_{r_{ak}^m}^2\right)/\sigma_z^2}\right). \tag{18}$$

The secret key capacity between Alice and the user in the transport area can be expressed as

$$I_t\left(h_k^{dl}; h_k^{ul}\right) = \log_2\left(1 + \frac{\left(\sigma_{h_{ak}}^2 + \sum_{m=M_r+1}^{M}\sigma_{r_{ak}^m}^2\right)^2/\sigma_z^4}{1 + 2\left(\sigma_{h_{ak}}^2 + \sum_{m=M_r+1}^{M}\sigma_{r_{ak}^m}^2\right)/\sigma_z^2}\right). \tag{19}$$

It can be seen from Eq. (10), Eq. (13) and Eq. (14) that the secret key capacity between Alice and the user can be changed by adjusting the coefficient β_m of STAR-RIS element, or it can be concluded that the key capacity between Alice and the user will be affected by the number of reflection mode elements M_r and the number of transmission mode elements M_t. In this section, it is necessary to effectively adjust the coefficient β_m of STAR-RIS elements to change the number of reflection mode elements M_r and the number of transmission mode elements M_t to maximize the secret key capacity in the entire system. Thus, the original problem can be further transformed into

$$\begin{aligned} OP_{1-1}: \max C_{sum} &= \sum_{k=1}^{p} I_r\left(h_k^{dl}; h_k^{ul}\right) + \sum_{k=1}^{q} I_t\left(h_k^{dl}; h_k^{ul}\right) \\ \text{s.t. } & M_r + M_t \leq M. \end{aligned} \tag{20}$$

In addition, assigning an attribute value η_k [26] to each user, where $\sum_{k=1}^{K} \eta_k = 1$, the weighted secret key capacity sum in the whole system can be obtained by

$$\begin{aligned} OP_{1-2}: \max C_{sum} &= \sum_{k=1}^{p} \eta_k I_r\left(h_k^{dl}; h_k^{ul}\right) + \sum_{k=1}^{q} \eta_k I_t\left(h_k^{dl}; h_k^{ul}\right) \\ \text{s.t. } & M_r + M_t \leq M. \end{aligned} \tag{21}$$

When the eavesdropping channel is related to the legitimate channel, the lower bound of the secret key capacity C_{LB} can be optimized to improve the “short board” of the overall secret key capacity of the system.

$$\begin{aligned} OP_{1-3}: \max C_{sum} &= \sum_{k=1}^{p} C_{LB,k}^{r} + \sum_{k=1}^{q} C_{LB,k}^{t} \\ \text{s.t. } & M_r + M_t \leq M. \end{aligned} \tag{22}$$

where $C_{LB,k}^{r}$ represents the lower bound of the secret key capacity between Alice and the user k located in the reflection region and $C_{LB,k}^{t}$ represents the lower bound of the secret key capacity between Alice and the user k located in the transport region.

3.2 Secret key capacity optimization under ES protocol

Under the ES protocol, all elements work in both reflection and transmission modes, and the reflection and transmission coefficient matrix follows the definition in Sect. 2. According to Eq. (10), the secret key capacity of Alice and the user in the reflection region can be refined as

$$I_r\left(h_k^{dl}; h_k^{ul}\right) = \log_2\left(1 + \frac{\left(\sigma_{h_{ak}}^2 + \sum_{m=1}^{M} \beta_m^r \sigma_{r_{ak}^m}^2\right)^2 / \sigma_z^4}{1 + 2\left(\sigma_{h_{ak}}^2 + \sum_{m=1}^{M} \beta_m^r \sigma_{r_{ak}^m}^2\right) / \sigma_z^2}\right). \tag{23}$$

The secret key capacity between Alice and the user in the transport area can be defined as

$$I_t\left(h_k^{dl};h_k^{ul}\right)=\log_2\left(1+\frac{\left(\sigma_{h_{ak}}^2+\sum_{m=1}^{M}\beta_m^t\sigma_{r_{ak}^m}^2\right)^2/\sigma_z^4}{1+2\left(\sigma_{h_{ak}}^2+\sum_{m=1}^{M}\beta_m^t\sigma_{r_{ak}^m}^2\right)/\sigma_z^2}\right). \tag{24}$$

When STAR-RIS is operating under the ES protocol, the reflection and transmission ratio of each element of STAR-RIS to the incident signal $\beta_m^r:\beta_m^t$ can be adjusted to maximize the sum of the secret key capacity in the whole system. The optimization problem of the sum of the secret key capacity in the whole system can be expressed as

$$\begin{aligned} OP_{2-1}:\max C_{sum}=\sum_{k=1}^{p}I_r\left(h_k^{dl};h_k^{ul}\right)+\sum_{k=1}^{q}I_t\left(h_k^{dl};h_k^{ul}\right)\\ \text{s.t. } \beta_m^r,\beta_m^t\in[0,1],\beta_m^r+\beta_m^t=1. \end{aligned} \tag{25}$$

3.3 Secret key capacity optimization under TS protocol

Under the TS protocol, a coherent time T_c is divided into $L=T_c/T_s$ time slots, in which L_r time slots STAR-RIS work in reflection mode and L_t time slots STAR-RIS work in transmission mode: $L_r+L_t=L$. The time slot division in channel probing is shown in Fig. 4. STAR-RIS operates in L_r time slots in reflection mode, and Alice can complete $b_r=L_r/2$ channel estimation with users in the reflected region (one time slot for downlink detection and one time slot for uplink detection). Similarly, Alice can perform $b_t=L_t/2$ channel estimation with users in the transport area. According to Eq. (10), the secret key capacity of Alice and the user in the reflection region and the transmission region can be expressed as

$$\begin{aligned} I(h_k^{dl};h_k^{ul})&=I_r(h_k^{dl};h_k^{ul})=I_t(h_k^{dl};h_k^{ul})\\ &=\log_2\left(1+\frac{(\sigma_{h_{ak}}^2+\sum_{m=1}^{M}\sigma_{r_{ak}}^2)^2/\sigma_z^4}{1+2(\sigma_{h_{ak}}^2+\sum_{m=1}^{M}\sigma_{r_{ak}}^2)/\sigma_z^2}\right). \end{aligned} \tag{26}$$

When STAR-RIS is working under the TS protocol, the ratio of time slots between STAR-RIS working in the reflection mode and the transmission mode $L_r:L_t$ can be adjusted to maximize the sum of the secret key capacity in the whole system. The

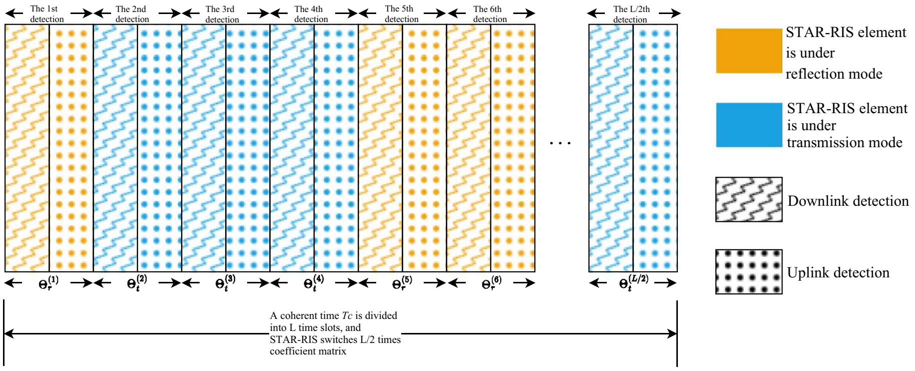


Fig. 4 Channel probing slot allocation for STAR-RIS auxiliary system under TS protocol

optimization problem of the sum of the secret key capacity in the whole system can be expressed as follows:

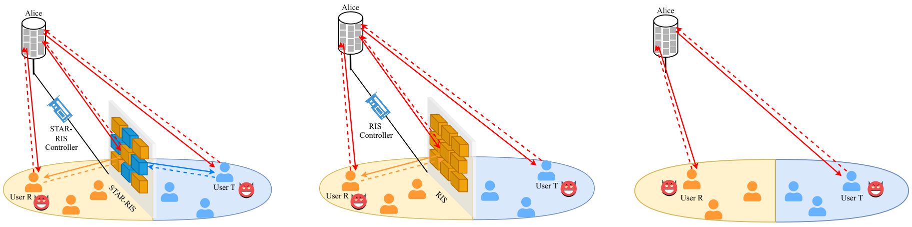
$$\begin{aligned} OP_{3-1}: \max C_{sum} &= \frac{1}{T_c}\left(b_r \sum_{k=1}^{p} I_r\left(h_k^{dl}; h_k^{ul}\right) + \sum_{k=1}^{q} b_t\left(z_k^{dl}; z_k^{ul}\right)\right) \\ \text{s.t. } b_r + b_t &= \frac{T_c}{2T_s}. \end{aligned} \tag{27}$$

4 Results and discussion

4.1 Secret key capacity

This section presents some numerical results for secret key capacity and verifies the derived numerical results through Monte Carlo simulation experiments [27]. In the simulation experiment, we use the ITE toolbox [28] to calculate mutual information. For all the images in this section, the dotted line represents the numerical result and the solid line represents the simulation result. The channel variance is $\sigma_h^2 = \beta_0 (d/d_0)^{-\zeta}$, where $\beta_0 = 30$ dB is the path loss at $d_0 = 1$ m, d is the link distance and ζ is the path loss coefficient (usually set to 4 in quasi-static environments). The transmitting power of the pilot signal is 20 dBm, the wavelength is 0.3 m, and the noise power is −96 dBm. There are 8 types of phase changes applied by STAR-RIS to the signal. This section also selected another two scenarios as the benchmark scheme, namely the RIS-assisted system [29] and the system [30] without RIS, as shown in Fig. 5. The RIS-assisted system is to increase the key capacity by RIS which can only reflect or transmit the incident signal. The primitive system does not use any auxiliary tools to generate keys.

Figure 6 shows the secret key capacity of the three physical layer key generation systems under different signal-to-noise ratios (SNRs). In Fig. 6, a user k_R is set in the reflection region with an attribute value $\eta_{k_R} = 0.3$ and a user k_T in the transmission region with an attribute value $\eta_{k_T} = 0.7$. In MS protocol, the secret key capacity of the system is $C_{\text{sum}} = \eta_{k_R} I_r\left(h_{k_R}^{dl}; h_{k_R}^{ul}\right) + \eta_{k_T} I_t\left(h_{k_T}^{dl}; h_{k_T}^{ul}\right)$. The number of elements of both STAR-RIS and RIS M is 64. STAR-RIS works under the MS protocol. When a user is located in the reflection blind area of RIS (such as the scene in Fig. 5-b), then the user in the blind area cannot get the artificial randomness brought by RIS. RIS can only serve the user k_R in the reflection area, while the user k_T in the blind area can only conduct channel probing with Alice through a direct channel. Therefore, the secret key capacity of the whole system is reduced. For example, when SNR is set to 20 dB,



(a) STAR-RIS assisted system (b) RIS assisted system (c) Primitive system

Fig. 5 Three kinds of physical layer key generation system models

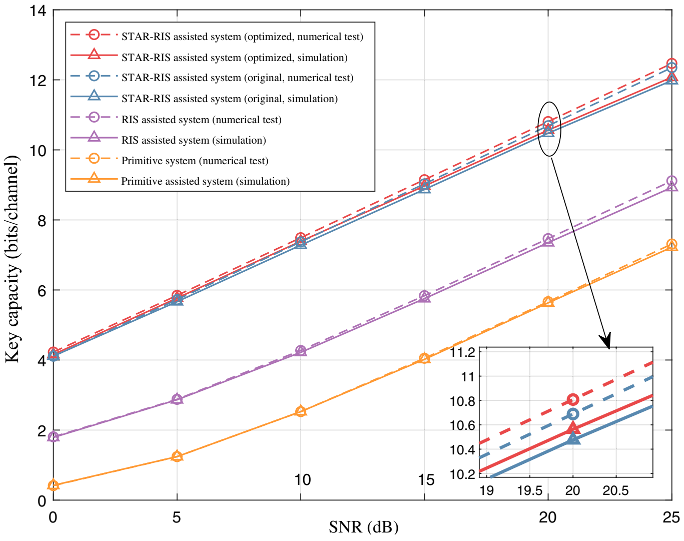


Fig. 6 Comparison of SKC variation with SNR in three systems

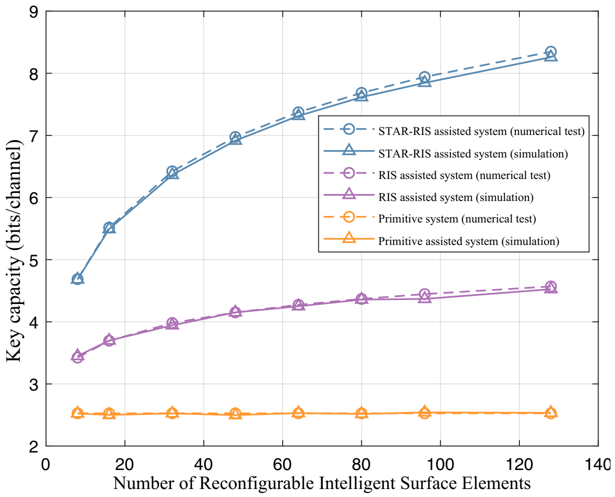


Fig. 7 Comparison of SKC with the number of elements in three systems

the secret key capacity of STAR-RIS auxiliary system increases by 44.76% and 90.76%, respectively, compared with RIS auxiliary system and without RIS auxiliary system. It is also observed that because the user k_R and the user k_T have different attribute values, it is possible to assign the number of reflection mode elements M_r and the number of transport mode elements M_t by optimizing the OP_{1-2} problem, thus obtaining a higher secret key capacity than the average allocation ($M_r = M_t = 32$) scheme.

Figure 7 compares the secret key capacity of each system under a different number of RIS elements. Here SNR is set to 10 dB, the attribute values of user k_R and user k_T are consistent with those set in Fig. 6, and STAR-RIS works under MS protocol. When the number of elements on the RIS rises, the secret key capacity of both the STAR-RIS auxiliary system and the RIS auxiliary system is increased. With the increase in the number of elements on the RIS, the number of available sub-channels increases, which can bring more secret key capacity. It should be noted that STAR-RIS-assisted systems are able to obtain the highest secret key capacity.

Figure 8 describes the secret key capacity of each system under different user numbers. SNR is set to 10 dB, the secret key capacity is calculated according to the expression defined in OP_{1-1} optimization rule, the number of elements of both STAR-RIS and RIS is 64, and STAR-RIS works under the MS protocol. From the results, we can find that the STAR-RIS-assisted system achieves the highest secret key capacity. As can be seen in Figs. 7 and 8, for a higher number of elements and users, the gap between the STAR-RIS-assisted system and the other two schemes becomes larger. These results show that the advantages of STAR-RIS-assisted systems are more significant when the number of elements or users increases.

Figures 9 and 10 show the secret key capacity of STAR-RIS operating under the three protocols. The number of STAR-RIS elements in Fig. 9 is 64, SNR is set to 10 dB in Fig. 10, and in all the scenarios in Figs. 9 and 10, there are 2 users: 1 user in the reflection area and 1 user in the transmission area. When STAR-RIS is in ES protocol, the reflection and transmission ratio of elements to incident signal $\beta_m^r : \beta_m^t$ is set to 0.3:0.7. When STAR-RIS is in the TS protocol, the total time slot number L in a coherent time is set to 200, and the time slot ratio of STAR-RIS working in reflection mode and transmission mode $L_r : L_t$ is set to 60:140. In this case, the weighted secret key capacity of the system can be expressed as $C_{\text{sum}} = \left(\frac{L_r}{2} I_r \left(h_{k_R}^{dl}; h_{k_R}^{ul} \right) + \frac{L_t}{2} I_t \left(h_{k_T}^{dl}; h_{k_T}^{ul} \right) \right) / \frac{L}{2}$. The first thing that can be observed from the image is that the TS protocol can bring higher secret key capacity than the other two working protocols. In the TS protocol, all surface elements of STAR-RIS can serve themselves regardless of whether the user is in the reflection region or the transmission region through the time slot switching method. Unlike ES protocol or

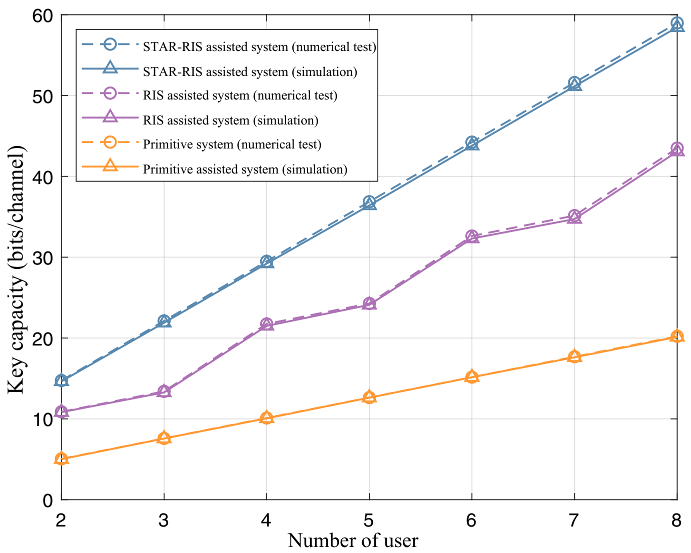


Fig. 8 Comparison of SKC with the number of users in three systems

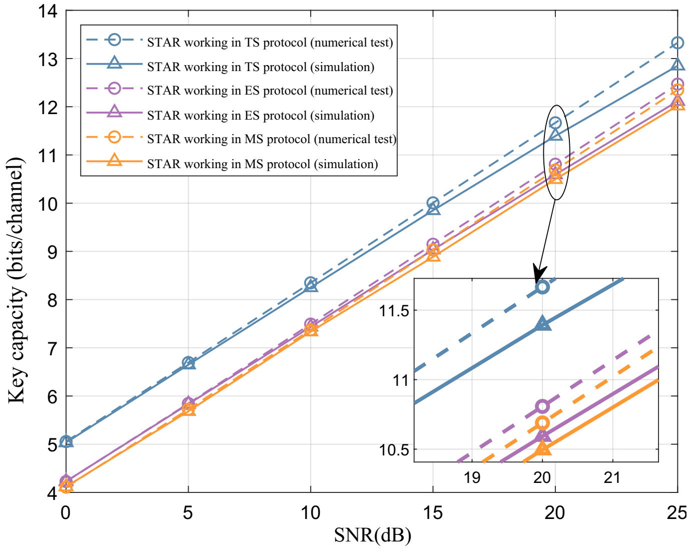


Fig. 9 Relationship between SKC and SNR of STAR-RIS under three working protocols

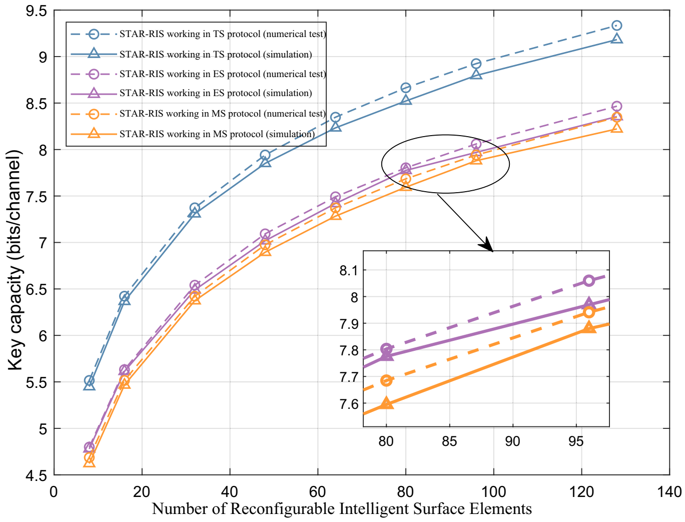


Fig. 10 Relationship between the SKC and the number of elements under three working protocols of STAR-RIS

MS protocol, part of STAR-RIS resources are reserved for users in other areas, so TS protocol can bring the highest secret key capacity.

Finally, Fig. 11 shows the influence on the secret key capacity of STAR-RIS system when the eavesdropper is less than half wavelength away from the user, where the number of STAR-RIS elements M is 64, STAR-RIS works under the MS protocol, there is a user k_R in the reflection area, its attribute value $\eta_{k_R} = 0.3$, and there is a user k_T in the transmission area and its attribute value $\eta_{k_T} = 0.7$. In the figure, the mutual information between Alice and the user refers to the secret key capacity when the distance between the listener and the user is greater than half wavelength. The upper and lower bounds of the secret key capacity show the range of the secret key capacity when the distance

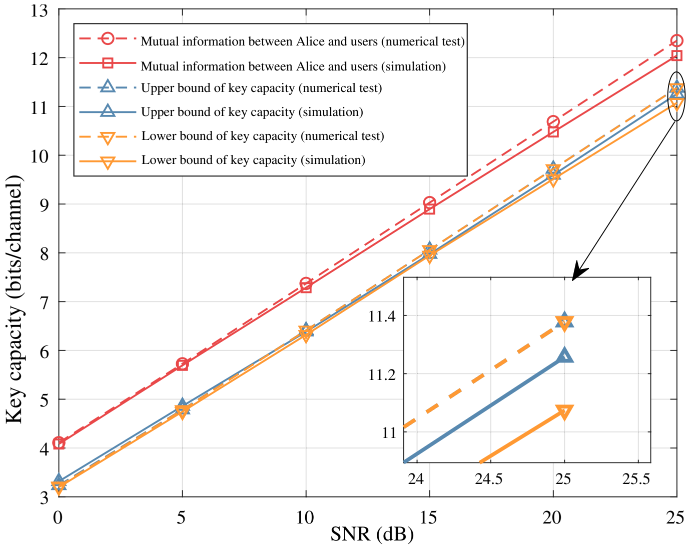


Fig. 11 SKC of STAR-RIS system at different SNR (there is a correlation between eavesdropping and legitimate channel)

between the listener and the user is less than half wavelength. The interception channel is modeled as $h_{ae} = \rho h_{ab} + \sqrt{1-\rho^2}$, where $\rho = J_0(2\pi d_{be}/\lambda), J_0(\cdot)$ is the first zero-order Bessel function, d_{be} is the distance between the antenna of Bob and Eve, $\omega \sim CN\left(0, \sigma_{ae}^2\right)$, the correlation between the listening channel and the legitimate channel $|\rho|$=0.7. When the eavesdropper is 0.054m away from the user, the correlation between the eavesdropper channel and the legitimate channel decreases the secret key capacity by 0.95 bits/channel (11.54%). In addition, as can be seen from the graph, the upper and lower bounds of the secret key capacity almost fit together, especially the numerical results.

4.2 Key inconsistency rate

The key inconsistency rate is the ratio of bits number of Alice that differ from primary key bits string generated by users to the total length of bits string. Figure 12 shows the curve of key inconsistency rate between users in STAR-RIS and traditional RIS systems as a function of SNR, in which the number of elements of both STAR-RIS and RIS is 64 and the number of elements working under MS protocol and reflection and transmission modes are 32, respectively. Bob is the user in the reflection space, Carol is the user in the transmission space, and Eve is an eavesdropper in the transmission space. The distance between the antenna of Eve and Carol is d_{be}=0.073 m, and the correlation coefficient $\rho = 0.5$. According to the results, traditional RIS can provide the lowest key inconsistency rate for user Bob, due to the fact that it provides twice the number of reflected channels compared to STAR-RIS. However, traditional RIS did not reduce Carol's key inconsistency rate. In addition, the key inconsistency rate of users Bob and Carol on both sides of STAR-RIS is similar, so the use of STAR-RIS brings more equitable key generation performance improvement. In terms of the inconsistent rate of key generation between user Carol and eavesdropper Eve, the curve shows that STAR-RIS-based assisted systems are more secure than traditional

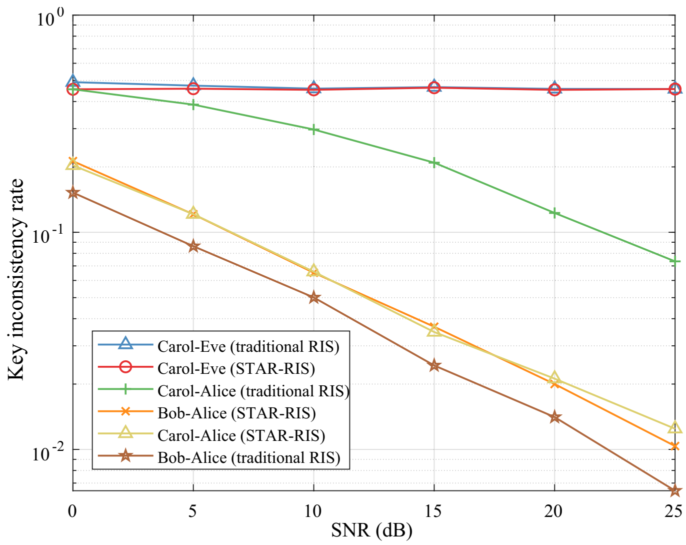


Fig. 12 Comparison of key inconsistency rates between users in STAR-RIS and traditional RIS systems

RIS. Despite the poor channel conditions leading to a high key inconsistency rate between Alice and Carol, there still exists a significant gap between the key inconsistency rate between Alice and Carol and that of the eavesdropper Eve. Therefore, a STAR-RIS-based system can guarantee the security of all legitimate user-generated keys in a low-signal-to-noise-ratio environment.

5 Conclusion

In this paper, a physical layer key generation system with STAR-RIS is designed. The number of sub-channels in the electromagnetic space is increased by STAR-RIS elements, and the performance of key generation for all users is improved. Moreover, the secret key capacity expressions of STAR-RIS under three different protocols are derived, and the optimization model of the secret key capacity under STAR-RIS is further analyzed. The simulation results not only prove the feasibility of using STAR-RIS to assist physical layer key generation but also show that STAR-RIS can greatly improve the performance of physical layer key generation.

Abbreviations

STAR-RIS	Simultaneous transmission and reflection reconfigurable intelligent surface
SKC	Secret key capacity
KGR	Key generation rate
RIS	Reconfigurable intelligent surface
PLS	Physical layer security
RSMA	Rate-splitting multiple access
CSCG	Circularly symmetric complex Gaussian distribution
MS	Mode switching and energy switching (ES)
TS	Time switching
ES	Energy switching
UT	User terminals
TDD	Time-division duplex

Acknowledgements
Not applicable.

Author Contributions

Each author made an equal contribution to the conceptualization, development, numerical simulations and composition of the manuscript. All authors have reviewed and given their approval to the final version of the manuscript.

Funding

The work was in part supported by the National Natural Science Foundation of China (No. U22B2026) and partly supported by the National Key Research and Development Program of China under Grant ID 2020YFE0200600.

Availability of data and materials

Not applicable.

Declarations

Competing interest

The authors declare that they have no conflict of interest.

Received: 22 March 2024 Accepted: 8 July 2024
Published online: 15 July 2024

References

1. K. Zeng, Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun. Mag. **53**(6), 33–39 (2015)
2. Y. Chen, Z. Chen, Y. Zhang, Z. Luo, Y. Li, B. Xing, B. Guo, L. Chen, Physical layer key generation scheme for mimo system based on feature fusion autoencoder. IEEE Internet Things J. **10**(16), 14886–14895 (2023)
3. M.A. Shawky, M. Bottarelli, G. Epiphaniou, P. Karadimas, An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks. IEEE Trans. Veh. Technol. **72**(7), 8738–8754 (2023)
4. N. Aldaghri, H. Mahdavifar, Physical layer secret key generation in static environments. IEEE Trans. Inf. Forensics Secur. **15**, 2692–2705 (2020)
5. L. Chen, Y. Lu, T. Lu, Z. Chen, A. Hu, et al. Wireless key generation scheme based on random permutation and perturbation in quasistatic environments. Wirel. Commun. Mobile Comput. (2023)
6. Y. Liu, J. Yang, K. Huang, X. Hu, Y. Wang, F. Wu, An optimal RIS design strategy for jointly improving key rate and communication performance in quasi-static environments. IEEE Wirel. Commun. Lett. **12**(9), 1618–1622 (2023)
7. Q. Cheng, L. Zhang, J.Y. Dai, W. Tang, J.C. Ke, S. Liu, J.C. Liang, S. Jin, T.J. Cui, Reconfigurable intelligent surfaces: simplified-architecture transmitters—from theory to implementations. Proc. IEEE **110**(9), 1266–1289 (2022)
8. K. Wang, P. Liu, K. Liu, L. Chen, H. Shin, T.Q. Quek, Joint beamforming and phase-shifting design for energy efficiency in ris-assisted miso communication with statistical csi. Phys. Commun. **59**, 102080 (2023)
9. C. Pan, G. Zhou, K. Zhi, S. Hong, T. Wu, Y. Pan, H. Ren, M. Di Renzo, A.L. Swindlehurst, R. Zhang et al., An overview of signal processing techniques for RIS/IRS-aided wireless systems. IEEE J. Sel. Top. Signal Process. **16**(5), 883–917 (2022)
10. L. Jin, X. Xu, S. Han, J. Liu, R. Meng, H. Chen, RIS-assisted physical layer key generation and transmit power minimization, in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2065–2070 (2022)
11. L. Jiao, G. Sun, J. Le, K. Zeng, Machine learning-assisted wireless phy key generation with reconfigurable intelligent surfaces, in *Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning*, 61–66 (2021)
12. Y. Yang, B. Zheng, S. Zhang, R. Zhang, Intelligent reflecting surface meets OFDM: Protocol design and rate maximization. IEEE Trans. Commun. **68**(7), 4522–4535 (2020)
13. F. Tan, X. Xu, H. Chen, S. Li, Energy-efficient beamforming optimization for miso communication based on reconfigurable intelligent surface. Phys. Commun. **57**, 101996 (2023)
14. T. Lu, L. Chen, J. Zhang, C. Chen, A. Hu, Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation. IEEE Trans. Inf. Forensics Secur. **18**, 3251–3266 (2023)
15. Z. Ji, P.L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin et al., Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans. Veh. Technol. **70**(1), 1030–1034 (2021)
16. T. Lu, L. Chen, J. Zhang, K. Cao, A. Hu, Reconfigurable intelligent surface assisted secret key generation in quasi-static environments. IEEE Commun. Lett. **26**(2), 244–248 (2021)
17. G. Li, C. Sun, W. Xu, M. Di Renzo, A. Hu, On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems. IEEE Trans. Inf. Forensics Secur. **17**, 211–225 (2021)
18. X. Mu, Y. Liu, L. Guo, J. Lin, R. Schober, Simultaneously transmitting and reflecting (star) RIS aided wireless communications. IEEE Trans. Wirel. Commun. **21**(5), 3083–3098 (2022)
19. Z. Chen, X. Ma, C. Han, Q. Wen, Towards intelligent reflecting surface empowered 6g terahertz communications: A survey. China Commun. **18**(5), 93–119 (2021)
20. F. Xiao, P. Chen, S. Xu, X. Pang, H. Liu, Physical layer security of star-RIS-aided RSMA systems. Phys. Commun. **61**, 102192 (2023)
21. Y. Liu, X. Mu, J. Xu, R. Schober, Y. Hao, H.V. Poor, L. Hanzo, Star: simultaneous transmission and reflection for 360° coverage by intelligent surfaces. IEEE Wirel. Commun. **28**(6), 102–109 (2021)
22. J. Xu, X. Mu, J.T. Zhou, Y. Liu, Simultaneously transmitting and reflecting (star)-riss: Are they applicable to dual-sided incidence? IEEE Wirel. Commun. Lett. **12**(1), 129–133 (2023)
23. H. Boche, R.F. Schaefer, H.V. Poor, On the computability of the secret key capacity under rate constraints, in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2427–2431 (2019)

24. Y. Wei, K. Zeng, P. Mohapatra, Adaptive wireless channel probing for shared key generation based on pid controller. IEEE Trans. Mob. Comput. **12**(9), 1842–1852 (2013)
25. M. Bloch, J. Barros, Physical-layer Security: from Information Theory to Security Engineering (2011)
26. F. Rottenberg, Optimal downlink training sequence for massive mimo secret-key generation, in *2021 IEEE 22nd International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 41–45 (2021)
27. P. Paxton, P.J. Curran, K.A. Bollen, J. Kirby, F. Chen, Monte Carlo experiments: design and implementation. Struct. Equ. Model. **8**(2), 287–312 (2001)
28. Z. Szabó, Information theoretical estimators toolbox. J. Mach. Learn. Res. **15**(1), 283–287 (2014)
29. X. Lu, J. Lei, Y. Shi, W. Li, Intelligent reflecting surface assisted secret key generation. IEEE Signal Process. Lett. **28**, 1036–1040 (2021)
30. H. Zhao, Y. Zhang, X. Huang, Y. Xiang, C. Su, A physical-layer key generation approach based on received signal strength in smart homes. IEEE Internet Things J. **9**(7), 4917–4927 (2022)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.