中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 253–269
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

静态场景下基于 RIS 天线的物理层密钥生成方案

杨杰[1,2], 季新生[1,2*], 黄开枝[1,2], 赵见磊[2], 管新荣[3]

1. 国家数字交换系统工程技术研究中心, 郑州 450002
2. 网络通信与安全紫金山实验室, 南京 211189
3. 陆军工程大学通信工程学院, 南京 210007
* 通信作者. E-mail: jxs_ndsc@126.com

收稿日期: 2021–08–25; 修回日期: 2021–09–30; 接受日期: 2021–10–25; 网络出版日期: 2022–01–29

国家重点研发计划课题 (批准号: 2020YFB1806607)、国家自然科学基金 (批准号: 61871404, 62171461) 及重点院校和重点学科专业建设项目资助

摘要 针对静态环境下密钥容量低的问题, 首次将 RIS 天线配置在基站设备端用于密钥生成, 通过捷变控制 RIS 单元相移变化, 生成随机快变波束, 并与原通信信道合并构成新的等价通信信道, 从而使密钥容量不受制于自然信道变化速度. 然后推导了该方案下密钥容量闭式解, 理论分析及仿真表明使用有限单元即可达到与快变信道环境下同等性能, 相较于 RIS 作为反射面部署的方案, 在密钥容量增益和防信息泄露等方面具有明显优势. 为进一步发挥 RIS 增益, 提出将部分单元用于密钥生成, 部分单元用于波束赋形的联合设计方案, 推导了该方案下闭式解. 最后, 在满足密钥容量和通信性能的基础上, 给出了最优资源分配策略, 仿真表明可以实现密钥容量与通信性能联合提升.

关键词 智能超表面, 密钥生成, 物理层安全, 静态场景, 资源分配

1 引言

物理层密钥生成技术是一种以无线信道特征作为随机源生成密钥的安全技术. 该技术为无线通信提供了一种轻量级的加密手段, 被认为是未来 6G 安全的增强技术之一 [1]. 然而在静态场景下, 如在智能家居、环境监测等物联网应用中, 信道变化十分缓慢, 密钥源随机性差, 无法满足密钥更新需求. 如何提升静态场景的密钥速率一直是密钥生成中亟待解决的问题之一 [2]. 现有的方法主要有中继辅助 [3]、人工引入随机信号 [4,5] 等方法. 这些方法虽然可以提升密钥速率, 但需要改动通信协议或部署额外的可信节点, 实际应用存在局限性.

近年来, 智能超表面 (reconfigurable intelligent surface, RIS) 因为其能够灵活操控无线信道的电磁特性, 一经出现就引起了广泛的关注, 有望成为 6G 网络中一项关键技术 [6]. 智能超表面由大量精心设计的电磁单元排列组成, 通过给电磁单元上的可调元件施加控制信号, 可以动态地调节这些单元的

引用格式: 杨杰, 季新生, 黄开枝, 等. 静态场景下基于 RIS 天线的物理层密钥生成方案. 中国科学: 信息科学, 2022, 52: 253–269, doi: 10.1360/SSI-2021-0295
Yang J, Ji X S, Huang K Z, et al. Secret key generation scheme based on RIS antenna for static environments (in Chinese). Sci Sin Inform, 2022, 52: 253–269, doi: 10.1360/SSI-2021-0295

电磁性质, 进而可以对入射信号的幅度、相位、极化等进行主动的智能调控. 作为超材料的二维实现, RIS 还具有成本低、易于共形等特性. RIS 引入无线通信网络, 提升原有信道的动态性和随机性, 为密钥生成技术的发展提供新的机会. 文献 [7] 提出将 RIS 部署在用户附近, 利用统计信道信息, 设计反射相移, 拉大合法与窃听信道差异, 从而提高密钥容量. 文献 [8] 通过随机设置 RIS 反射相移, 提升反射信道的随机性, 从而提高静态环境的密钥容量; 进一步, 文献 [9] 利用 RIS 和商业 Wi-Fi 设备搭建一套原型系统, 验证了方案有效性. 然而, 上述研究均是将 RIS 作为反射面部署在无线环境中, 由于 RIS 自身是无源的, 当位置部署不当, 受大尺度损耗影响, 引入的反射路径相对直射径增益有限.

实际上, 智能超表面不仅能够用作反射面, 还可以作为辐射面安装在设备端替代传统阵列天线 [10]. 从通信角度考虑, 相较于高成本的相控阵天线, RIS 天线无需复杂的馈电相移网络, 即可实现模拟波束赋形. 文献 [11] 将 RIS 天线应用于大规模 MIMO 系统, 并验证与理想阵列天线性能接近. 文献 [12] 提出了一种基于 RIS 天线的混合预编码架构, 并用深度学习算法给出应用于太赫兹通信的最优预编码方案. 而从安全角度考虑, RIS 整体作为一个面或多个子面, 通过捷变调控辐射单元相移, 等效为单个或多个低成本可控方向图的定向天线, 可获得更丰富无线信道特征. 当用于密钥生成, 通过调整随机变化的波束并与原信道级联可以产生时变的等价信道, 有望提高静态场景下密钥容量, 相关研究尚未有涉及.

基于上述分析, 本文在不改变现有设备协议基础上, 将 RIS 天线和控制器部署在基站设备端, 并将该架构首次应用于密钥生成, 通过随机快变辐射单元相移, 使得双方探测的信道在自然信道基础上叠加新的随机源, 进而实现密钥容量的提升. 然后推导获得该方案的密钥容量, 相较于基于反射面的方案, 密钥容量显著提升, 且引入随机源不会对窃听方带来信息泄露. 进一步, 考虑到辐射单元数量增加到一定程度后, 密钥容量保持不变. 为充分发挥 RIS 增益, 给出了通信安全联合设计方案, 其中部分单元用于提升密钥容量, 部分单元用于波束赋形增强通信性能, 并推导了该方案下性能闭式解. 最后, 在给定 QoS (quality of service) 指标基础上, 给出了最优资源分配策略, 实现通信与安全性能联合提升.

2 密钥生成方案

2.1 方案描述

如图 1 所示, 我们给出了基于 RIS 天线的三节点密钥生成模型, 合法用户 Alice 和 Bob 正常通信, 利用无线信道特征生成密钥并对信息加密; Eve 部署位置距合法用户远大于几个波长, 接收空口信号并尝试获取密钥解密信息. Alice 端安装 RIS 天线. RIS 天线由 N 个辐射单元组成, 每个单元间信道相互独立, 并可独立对发射/接收信号进行相位调控. 与文献 [12] 采用的空间馈电连接方式不同, 一条射频链路与 N 个单元级联在一起, 采用微带线或波导等方式馈电, 并假定每个单元具有相同的频率选择性 [11]. 同时构造由 FPGA 设计的 RIS 控制器, 用于实时控制辐射单元相移. 基带电路与 RIS 控制器通过同步链路建立时序同步, 在每个子帧时隙, 控制 RIS 单元相位变化. Bob 和 Eve 均采用单天线接收/发射信号.

接下来给出基于 RIS 天线的密钥生成方案. 如图 2 所示, 主要包括相移随机、信道探测、密钥生成 3 个阶段.

(1) 相移随机: 在每一个子帧时隙开始前, Alice 通过 RIS 控制器随机调控 RIS 各辐射单元的相移, 需要说明的是该随机性不能预先设置, 否则 Eve 将获得一定信息量.

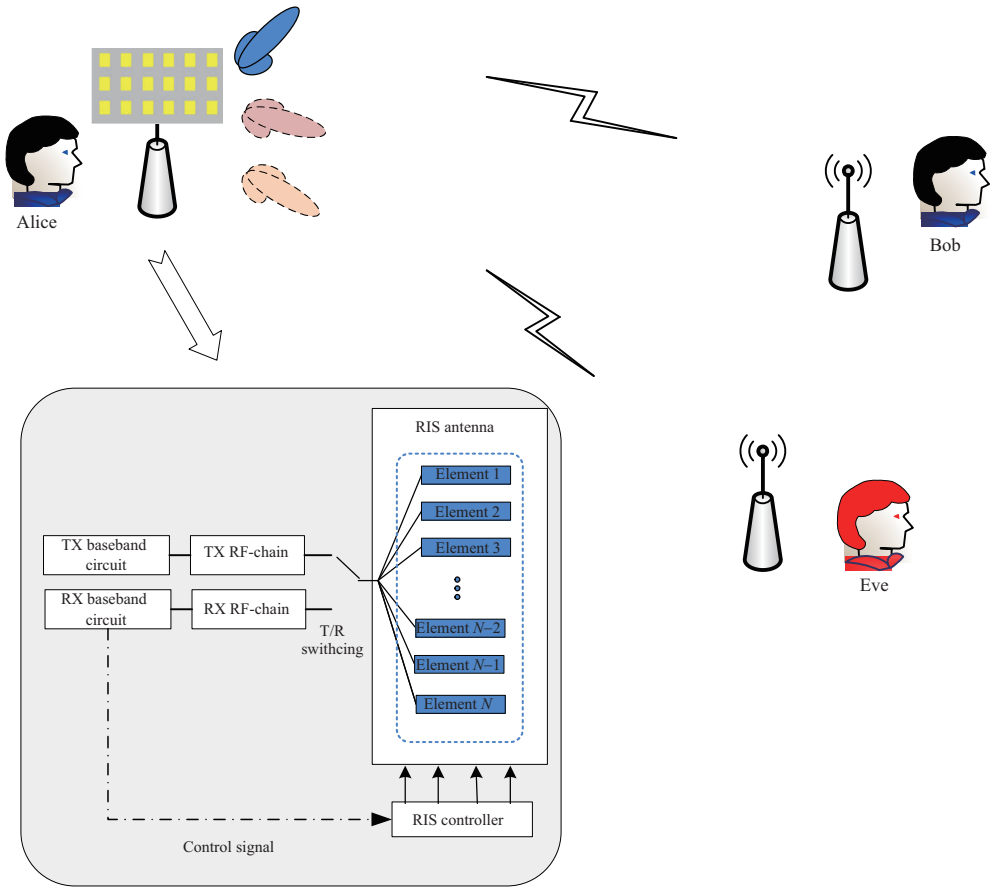

图 1　(网络版彩图) 基于 RIS 天线密钥生成模型

Figure 1　(Color online) Secret key generation model based on RIS antenna

(2) 信道探测: 在该阶段, Alice 和 Bob 分别互发导频进行信道估计, 提取相应链路的信道状态信息.

(3) 密钥生成: 首先采用均匀量化方案对信道估计值进行量化, 接着利用纠错编码方案纠正不一致的比特; 最后采用基于哈希函数的隐私放大算法来避免信息泄露. 通过上述过程, 通信双方完成相同的密钥建立. 该阶段不是本文的重点, 具体实现可参考文献 [13].

从实现流程上看, 本文的方案对于现有终端仅需做两处改动. 一是将普通天线换成 RIS 天线, 由于 RIS 具有低成本、易共形等特性, 所需代价较小, 且相较于电控无源阵列天线 (electronically steerable parasitic array radiator antenna, ESPAR) 辅助密钥生成方案 [14], RIS 工作频率宽、阵元间互耦影响小、信号建模简单; 二是基带电路送出同步信号至 RIS 控制器, 用于同步调整相移. 现有的两类基带侧引入随机源方案, 一类为保证数据传输阶段数据正确译码, 需要对通信双方的协议进行修改以及适配 [5]; 另一类需要单端配置多条射频链路以实现随机波束成形 [15], 所需成本高. 本文所提方案在射频前端引入随机性, 无需修改现有基带协议, 且仅需改造单端节点. 特别是对于有中心的物联网系统, 只需对中心节点的设备进行改造, 其余用户节点无需调整. 因而本文的方案易部署优势明显.

2.2　方案性能分析

接下来分析该方案对于密钥性能的提升. 无线信道用瑞利 (Rayleigh) 信道建模, Alice 到 Bob 和

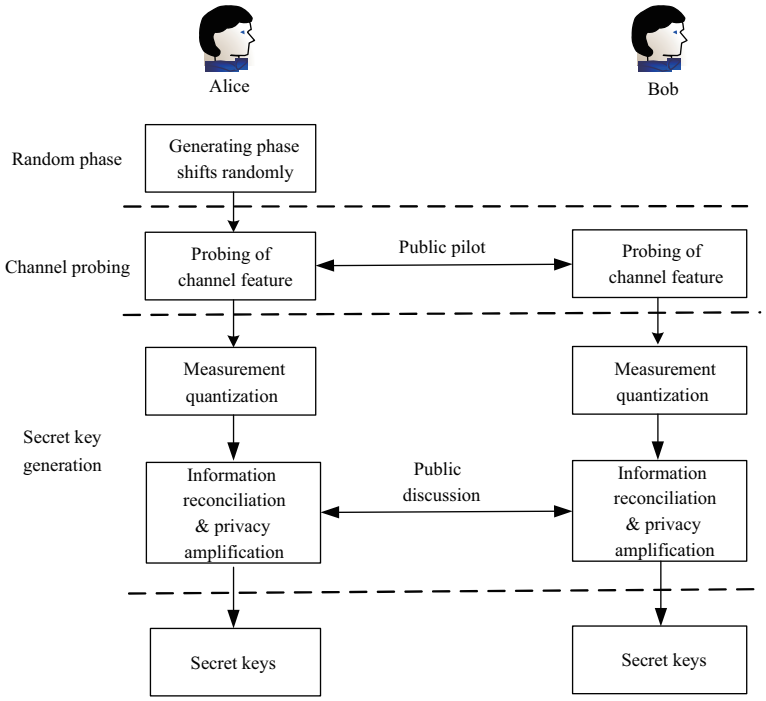

图 2　(网络版彩图) 基于 RIS 天线的密钥生成流程图

Figure 2　(Color online) Secret key generation flow chart based on RIS antenna

Eve 信道分别表示为 $\boldsymbol{h}_{\mathrm{ab}} \in \mathcal{C}^{N\times 1}$ 和 $\boldsymbol{h}_{\mathrm{ae}} \in \mathcal{C}^{N\times 1}$, Bob 到 Alice 的信道表示为 $\boldsymbol{h}_{\mathrm{ba}} \in \mathcal{C}^{N\times 1}$. 其中, 到达各天线单元子信道表示为 $h_{\mathrm{ab},n} \sim \mathcal{CN}(0,\sigma_{\mathrm{ab}}^2)$, $h_{\mathrm{ae},n} \sim \mathcal{CN}(0,\sigma_{\mathrm{ae}}^2)$ 和 $h_{\mathrm{ba},n} \sim \mathcal{CN}(0,\sigma_{\mathrm{ba}}^2)$. 由于上下行信道互易, 我们有 $\sigma_{\mathrm{ab}}^2 = \sigma_{\mathrm{ba}}^2$. 在第 i 次信道探测前, 相移向量随机设置为 $\boldsymbol{v}_i^{\mathrm{H}} = [\mathrm{e}^{\mathrm{j}\theta_{i,1}}, \mathrm{e}^{\mathrm{j}\theta_{i,2}}, \ldots, \mathrm{e}^{\mathrm{j}\theta_{i,N}}]$, 其中 $\theta_{i,n} \in [0, 2\pi]$ 服从连续均匀分布.

在 i 次上行探测时隙, Bob 发送的导频为 $\sqrt{P}\boldsymbol{s}$, 其中 P 表示发送功率, $\boldsymbol{s}$ 表示长度为 l_p 的导频序列, 则加装 RIS 天线后, Alice 端接收信号可表示为

$$\boldsymbol{y}_{\mathrm{a}} = \sum_n h_{\mathrm{ba},n}\mathrm{e}^{\mathrm{j}\theta_{i,n}}\sqrt{\frac{P}{N}}\boldsymbol{s} + \boldsymbol{n}_{\mathrm{a}} = \boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ba}}\sqrt{\frac{P}{N}}\boldsymbol{s} + \boldsymbol{n}_{\mathrm{a}}, \tag{1}$$

其中, $\boldsymbol{n}_{\mathrm{a}}$ 表示接收端加性高斯 (Gauss) 白噪声, 方差为 σ_n^2.

同样地, 在 i 次下行探测时隙, 使用相同的相移配置, Bob 或 Eve 的接收信号表示为

$$\begin{aligned}\boldsymbol{y}_{\mathrm{b}} &= \boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}}\sqrt{\frac{P}{N}}\boldsymbol{s} + \boldsymbol{n}_{\mathrm{b}},\\ \boldsymbol{y}_{\mathrm{e}} &= \boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ae}}\sqrt{\frac{P}{N}}\boldsymbol{s} + \boldsymbol{n}_{\mathrm{e}},\end{aligned} \tag{2}$$

其中, $\boldsymbol{n}_{\mathrm{b}}$ 和 $\boldsymbol{n}_{\mathrm{e}}$ 分别表示 Bob 和 Eve 端噪声, 假定与 Alice 使用同等类型设备, 噪声方差均为 σ_n^2.

可以看到, 相较于全向天线, 使用 RIS 天线, 等效于对子信道上进行相位加权合并, 合并效果相当于方向图可变的定向天线.

接着, 通信用户采用最小二乘法进行信道估计. 其中, Bob 获得的信道状态信息 $\widehat{h}_{\mathrm{ab}}$ 可表示为

$$\widehat{h}_{\mathrm{ab}} = \boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}} + n_{\mathrm{b}}', \tag{3}$$

其中 $n'_{\mathrm{b}}=\frac{\sqrt{\frac{P}{N}}\boldsymbol{s}^{\dagger}}{\|\sqrt{\frac{P}{N}}\boldsymbol{s}\|^2}\boldsymbol{n}_{\mathrm{b}}$.

其估计方差可表示为

$$\sigma^2_{\widehat{h}_{\mathrm{ab}}}=\sigma^2_{\boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}}}+\frac{\sigma_n^2}{\|\sqrt{\frac{P}{N}}\boldsymbol{s}\|^2}=\sigma^2_{\boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}}}+\frac{\sigma_n^2}{\frac{P}{N}l_p}. \tag{4}$$

对于变量 $Y=\boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}}=\sum\limits_n h_{\mathrm{ab},n}\mathrm{e}^{\mathrm{j}\theta_{i,n}}$, θ_n 服从独立均匀分布, $h_{\mathrm{ab},n}$ 独立但在静态环境下的分布无闭式解, 因而, 变量 Y 分布闭式解难以获得.

定理1 当辐射单元数量 N 足够大时, Y 服从高斯分布且在任意两个信道探测时隙独立.

证明 首先, 由于 $h_{\mathrm{ab},n}\mathrm{e}^{\mathrm{j}\theta_n}$, $\forall n$ 独立同分布, 当 N 足够大时, 利用中心极限定理 [16], 我们有 $Y\sim\mathcal{CN}(0,N\sigma^2_{\mathrm{ab}})$. 接着证明在任意第 j 和 k 次信道探测获得的 Y_j 和 Y_k 独立.

对于静态场景, 信道变化缓慢, 分两种情况讨论.

(1) 在第 j 和 k 次信道探测时, 信道不变, 即 $h_{\mathrm{ab},n,j}=h_{\mathrm{ab},n,k}$, $\forall n$, 则协方差可得

$$\begin{aligned}\mathrm{Cov}(Y_jY_k^*)&=\mathbb{E}\left(\sum_n h_{\mathrm{ab},n,j}\mathrm{e}^{\mathrm{j}\theta_n}\sum_m h^*_{\mathrm{ab},m,k}\mathrm{e}^{-\mathrm{j}\theta_m}\right)\\&\overset{\text{(a)}}{=}\mathbb{E}\left(\sum_n|h_{\mathrm{ab},n,j}|^2\mathrm{e}^{\mathrm{j}\theta_n-\mathrm{j}\theta_m}\right)\\&\overset{\text{(b)}}{=}0\overset{\text{(c)}}{=}\mathbb{E}(Y_j)\mathbb{E}(Y_k^*),\end{aligned} \tag{5}$$

其中, 由于 $\forall n\neq m$, $h_{\mathrm{ab},n,j}$ 和 $h_{\mathrm{ab},m,k}$ 独立, 等式 (a) 成立; 由于 θ_n 服从均匀分布, 等式 (b) 成立; 由于 $\forall j$, $\mathbb{E}(Y_j)=0$, 等式 (c) 成立.

(2) 在第 j 和 k 次信道探测时, 信道独立, 则易推得

$$\begin{aligned}\mathrm{Cov}(Y_jY_k^*)&=\mathbb{E}\left(\sum_n h_{\mathrm{ab},n,j}\mathrm{e}^{\mathrm{j}\theta_n}\sum_m h^*_{\mathrm{ab},m,k}\mathrm{e}^{-\mathrm{j}\theta_m}\right)\\&\overset{\text{(d)}}{=}0=\mathbb{E}(Y_j)\mathbb{E}(Y_k^*),\end{aligned} \tag{6}$$

其中, 由于 $\forall n,m$, $h_{ab,n,j}$ 和 $h_{ab,m,k}$ 独立, 等式 (d) 成立.

则可得 Y_j 和 Y_k 不相关. 由于高斯分布独立与不相关等价, 因而任意两次信道探测时隙获得的 Y_j 和 Y_k 独立, 即可得证.

进而, 可知 $\widehat{h}_{\mathrm{ab}}$ 服从高斯分布, 即通过 RIS 提供的大量单元使合并加权信道趋于高斯分布.

同样地, 可分别获得 Alice 和 Eve 的观测信道表达式

$$\widehat{h}_{\mathrm{ba}}=\boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ba}}+\frac{\sqrt{\frac{P}{N}}\boldsymbol{s}^{\dagger}}{\|\sqrt{\frac{P}{N}}\boldsymbol{s}\|^2}\boldsymbol{n}_{\mathrm{a}}, \tag{7}$$

$$\widehat{h}_{\mathrm{ae}}=\boldsymbol{v}_i^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ae}}+\frac{\sqrt{\frac{P}{N}}\boldsymbol{s}^{\dagger}}{\|\sqrt{\frac{P}{N}}\boldsymbol{s}\|^2}\boldsymbol{n}_{\mathrm{e}}. \tag{8}$$

同理, 利用中心极限定理, 可推得 $\widehat{h}_{\mathrm{ba}}$ 和 $\widehat{h}_{\mathrm{ae}}$ 服从高斯分布.

根据密钥容量的定义, 当考虑 Eve 存在时, 密钥容量可以表示为 [17]

$$C_{\mathrm{SK}}{=}I(\widehat{h}_{\mathrm{ab}},\widehat{h}_{\mathrm{ba}})-I(\widehat{h}_{\mathrm{ab}},\widehat{h}_{\mathrm{ae}}). \tag{9}$$

接下来分别求解 $I(\widehat{h}_{\mathrm{ab}},\widehat{h}_{\mathrm{ba}})$ 和 $I(\widehat{h}_{\mathrm{ab}},\widehat{h}_{\mathrm{ae}})$. 不失一般性, 仅考虑从 I 路提取信息, 即

$$I(\widehat{h}_{\mathrm{ab}},\widehat{h}_{\mathrm{ba}})=I(\widehat{h}_{\mathrm{ab},I};\widehat{h}_{\mathrm{ba},I}), \tag{10a}$$

$$\widehat{h}_{\mathrm{ab},I}=\sum_{n}\left(h_{\mathrm{ab},n,I}\cos\theta_{i,n}-h_{\mathrm{ab},n,Q}\sin\theta_{i,n}\right)+n'_{\mathrm{b},I}, \tag{10b}$$

$$\widehat{h}_{\mathrm{ba},I}=\sum_{n}\left(h_{\mathrm{ba},n,I}\cos\theta_{i,n}-h_{\mathrm{ba},n,Q}\sin\theta_{i,n}\right)+n'_{\mathrm{a},I}. \tag{10c}$$

易知 $\widehat{h}_{\mathrm{ab},I}$ 和 $\widehat{h}_{\mathrm{ba},I}$ 服从高斯分布, 其均值为 0, 方差为 $\sigma^2_{\boldsymbol{v}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{ab}}}+\frac{\sigma_n^2}{\frac{P}{N}l_p}$. 高斯随机变量的互信息可通过相关系数 $\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ba},I})$ 表示为

$$I(\widehat{h}_{\mathrm{ab},I};\widehat{h}_{\mathrm{ba},I})=-\frac{1}{2}\log_2(1-\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ba},I})^2). \tag{11}$$

由式 (10b) 和 (10c), 相关系数可推导为

$$\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ba},I})=\frac{\mathbb{E}\{\widehat{h}_{\mathrm{ab},I}\widehat{h}_{\mathrm{ba},I}\}}{\sqrt{\sigma_{\widehat{h}_{\mathrm{ba},I}}\sigma_{\widehat{h}_{\mathrm{ab},I}}}}=\frac{\sigma^2_{\mathrm{ab}}}{\sigma^2_{\mathrm{ab}}+\frac{\sigma_n^2}{\frac{P}{N}l_p}}. \tag{12}$$

下面分析 $\widehat{h}_{\mathrm{ab},I}$ 和 $\widehat{h}_{\mathrm{ae},I}$ 的互信息, $\widehat{h}_{\mathrm{ae},I}$ 表达式为

$$\widehat{h}_{\mathrm{ae},I}=\sum_{n}\left(h_{\mathrm{ae},n,I}\cos\theta_{i,n}-h_{\mathrm{ae},n,Q}\sin\theta_{i,n}\right)+n'_{\mathrm{e},I}. \tag{13}$$

易知 $\widehat{h}_{\mathrm{ae},I}$ 服从高斯分布, 则互信息 $I(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})$ 可表示为

$$I(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})=-\frac{1}{2}\log_2(1-\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})^2). \tag{14}$$

即转化为求解相关系数 $\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})$, 可推导得

$$\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})=\frac{\mathbb{E}\{\widehat{h}_{\mathrm{ab},I}\widehat{h}_{\mathrm{ae},I}\}}{\sqrt{\sigma_{\widehat{h}_{\mathrm{ab},I}}\sigma_{\widehat{h}_{\mathrm{ae},I}}}}=0. \tag{15}$$

即可得 $I(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ae},I})=0$. 这表明, 虽然 Eve 探测的信道中含有合法链路中的相移信息, 但并未获得任何信息量. 此外, 由于 Alice 仅有一条基带链路, 窃听者难以预先获得 $h_{\mathrm{ae},n}$, 因而对于窃听者来说, 通过拿到自然信道再反解获得人工随机源的方法将失效 [18]. 需要指出的是, 式 (14) 和 (15) 在 N 较大的情况下成立, 即需满足中心极限定理. 若考虑极限情况, 如 $N=1$ 时, 易知存在信息泄露. 后续将通过仿真进一步验证.

最后可得密钥容量

$$C_{\mathrm{SK}}=-\frac{1}{2}\log_2\left(1-\left(\frac{\sigma^2_{\mathrm{ab}}}{\sigma^2_{\mathrm{ab}}+\sigma_n^2/(Pl_p)}\right)^2\right). \tag{16}$$

与之对比的是, 在快变环境下, 即帧周期与相干时间相等, 密钥容量 C'_{SK} 为 [19]

$$C'_{\mathrm{SK}}=-\frac{1}{2}\log_2\left(1-\left(\frac{\sigma^2_{\mathrm{ab}}}{\sigma^2_{\mathrm{ab}}+\sigma_n^2/(Pl_p)}\right)^2\right). \tag{17}$$

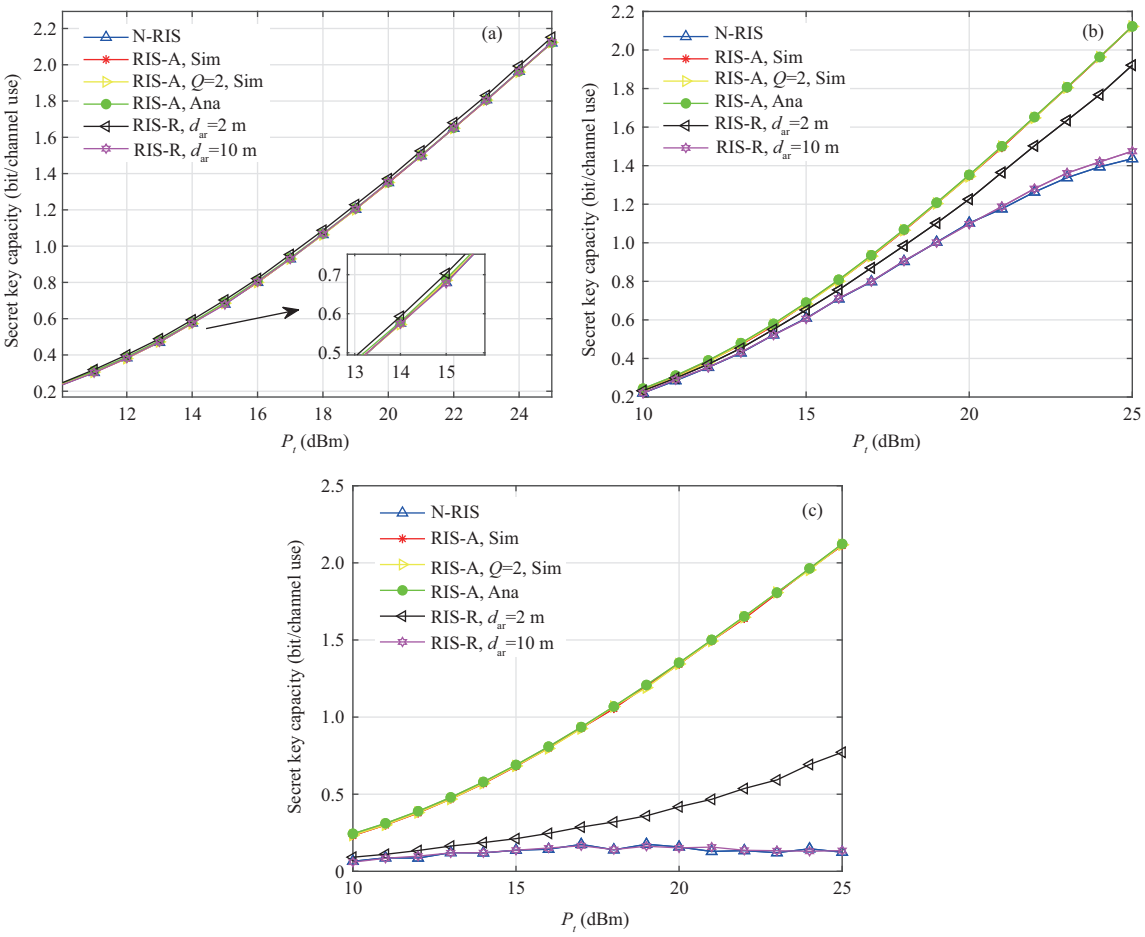

图 3　(网络版彩图) 不同发送功率下密钥容量 ($N = 30$)

Figure 3　(Color online) Secret key capacity versus transmit power ($N = 30$). (a) $T_c = 1$ ms; (b) $T_c = 50$ ms; (c) $T_c = 1$ s

比较式 (16) 和 (17), 可知 $C_{\mathrm{SK}} = C'_{\mathrm{SK}}$. 即通过引入 RIS 天线实现信道感知快变, 可提升密钥容量至与快变环境下一致. 我们知道, 在不增加发射功率等系统参数的情况下, 快变环境下密钥容量是性能上界, 从而进一步说明了所提方案的优势. 同时可知, 继续增加 N, 密钥容量并不能继续提升, 后续通过仿真进一步验证.

2.3　方案仿真验证

为验证上述理论分析, 采用蒙特卡罗 (Monte Carlo) 方法对所提方案 (记为 RIS-A) 仿真实验, 并利用 Information Theoretical Estimator (ITE) 工具箱计算互信息量. 系统参数配置为 Alice, Bob, Eve 分别位于坐标 $(0, 0)$, $(65, 0)$, $(40, 10)$ 处, 单位为 m. 路径衰落系数 $\chi = 3$, 参考路损 $L_0 = -30$ dB [20], 子帧周期设置为 1 ms, $\sigma_n^2 = -65$ dBm, $l_p = 10$. 作为比较, 给出基于 RIS 反射面方案 (记为 RIS-R) [8] 以及没有 RIS 的方案 (记为 N-RIS) 的性能, 其中为刻画 RIS 用作反射面部署于不同位置时的性能, 分别设置 RIS 靠近 Alice 部署 (0, 2) 以及 RIS 位于用户中间部署 (10, 0).

图 3 给出了不同发送功率以及不同相干时间 (记为 T_c) 下 3 种方案的性能对比. 可以看到, 随着发送功率的增加, 两种 RIS 方案的密钥容量均逐渐增加. 比较 3 个子图, 相较于 N-RIS 方案, 无论

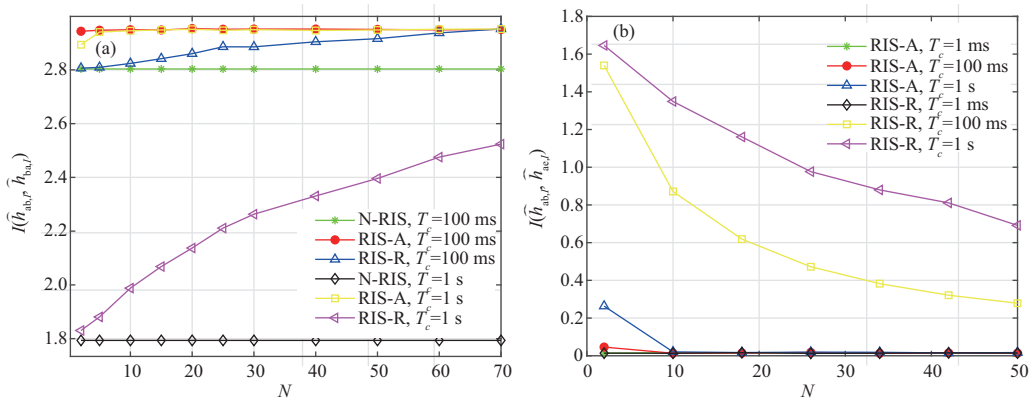

图 4 (网络版彩图) 不同辐射单元下互信息量 ($P = 30$ dB)

Figure 4 (Color online) Mutual information versus the number of radiating elements ($P = 30$ dB). (a) $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ba},I})$; (b) $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$

是 RIS-A 方案还是 RIS-R 方案密钥容量均得到提升, 说明 RIS 方案有助于提升静态环境密钥容量. 进一步可以看到, RIS-A 方案的性能与快变环境下的密钥容量一致, 且不随 T_c 增大而发生变化, 与理论分析一致, 说明本文所提方案能够有效克服慢变环境影响. 而对于 RIS-R 方案, 在快变环境下, 即 $T_c = 1$ ms, RIS-R 方案的密钥容量比其他方案略高, 这是由于部署 RIS 后引入的反射路径使得式 (16) 中的 σ_{ab}^2 增加, 然而当环境变化缓慢时, 即增大 T_c, 密钥容量迅速下降, 此时 RIS-A 方案性能最优. 这是由于 RIS-R 方案仅能使得反射路径变得随机, 信道中还存在占据主要成分的直达径, 因而密钥容量增加受限. 此外, 对于 RIS-R 方案, 当 RIS 部署距离 Alice 越远, 性能增益越小. 在图 3(c) 中, 当 $d_{ar} = 10$ m 时, 其性能与 N-RIS 方案基本一致, 这是由于反射路径损耗与 Alice-RIS 和 RIS-Bob 距离的乘积成正比 [21]. 当远离用户部署时, 引入反射级联路径增益很小, 进一步说明了 RIS-R 方案的局限性. 最后, 考虑到 RIS 硬件能力的限制, 实际中只能取离散相移. 图 3 中给出了 2 bit 量化下系统性能, 记为 RIS-A, $Q = 2$, 可以看到与连续取值的性能一样. 这是因为定理 1 的证明中仅要求相移服从均匀分布, 而与相移连续或离散取值无关.

图 4 分别给出互信息量 $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ba},I})$ 和 $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$ 随辐射单元数量和相干时间变化的性能, 其中 RIS-R 方案中 $d_{\mathrm{ar}} = 2$ m (后续仿真均按此配置). 从图 4(a) 中可以看到, 对于 RIS-A 方案, $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ba},I})$ 随着 N 增大而缓慢上升, 当 $N \geqslant 10$ 时, 密钥容量保持不变并达到性能界, 说明虽然定理 1 的证明要求 N 足够大, 但实际中仅需有限单元即可保证性能. 而对于 RIS-R 方案, $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ba},I})$ 随着 N 增大而上升, 当 $T_c = 100$ ms, $N \geqslant 70$ 时, 与 RIS-A 方案性能接近, 当 $T_c = 1$ s 时, 所需的单元数量更多, 即需要更多的维度来对静态信道随机调控. 从图 4(b) 中可以看到, 当 N 较小时, $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$ 较大, 即存在一定的信息泄露, 特别是在 T_c 较大时, 信息量泄露更多. 同等条件下, RIS-R 方案的 $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$ 更高, 即存在更大泄露风险. 而当通过增加 N, 在不同 T_c 下, $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$ 均逐渐下降趋近于 0, 信息泄露可以忽略, 且提出的 RIS-A 方案在相干时间很长时, 仍可以以较小 N 快速减小 $I(\widehat{h}_{\mathrm{ab},I}, \widehat{h}_{\mathrm{ae},I})$, 验证了 2.2 小节理论分析. 说明所提方案在实际应用时无需考虑窃听信道中含有相移信息所带来的信息泄露风险.

3 通信安全联合设计方案

第 2 小节给出的 RIS 天线增强密钥方案中, 当在射频前端配置 RIS 天线时, 通过随机设置相移,

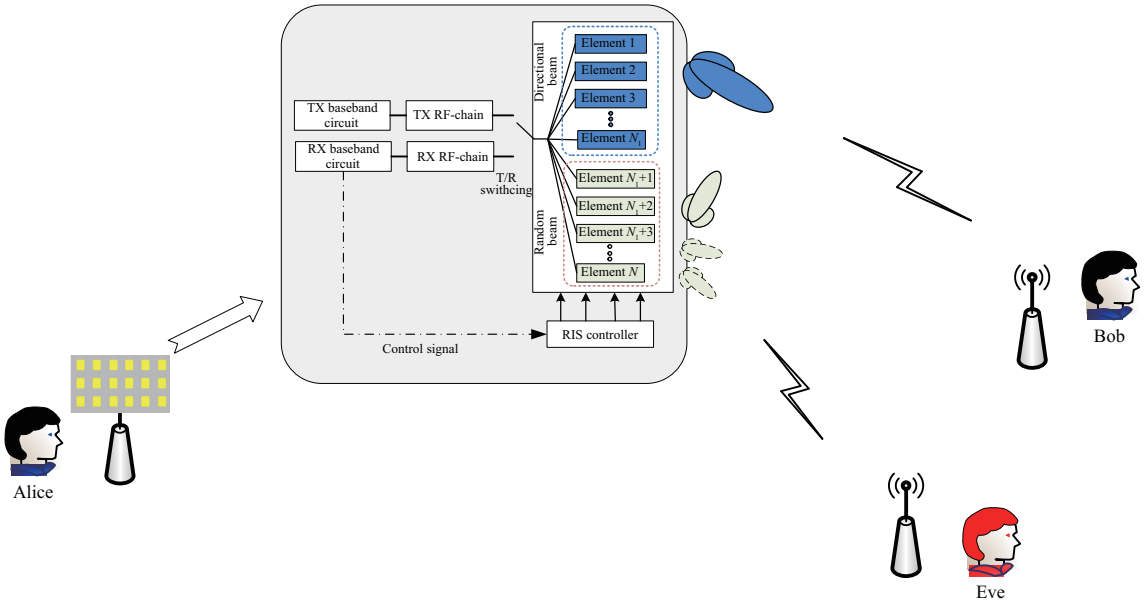

图 5 (网络版彩图) 基于 RIS 天线通信安全联合设计模型

Figure 5 (Color online) Communication and security integrated model based on RIS antenna

可显著提升静态环境下的密钥容量. 由理论及仿真分析可知, N 增大到一定程度时, 并不会再带来密钥性能增益. 因而, 可以考虑将余下的单元用于增强指定用户的通信性能, 从而进一步挖掘 RIS 天线带来的性能增益.

3.1 方案描述

基于此, 如图 5 所示, 提出一种基于 RIS 天线通信安全联合设计方案 (记为 RIS-U). 系统各节点配置与 RIS-A 方案一致, 不同的是, 一部分 RIS 单元用于构造随机可变定向天线, 用于密钥生成, 一部分 RIS 单元配置固定相移, 用于波束赋形. 帧周期记为 T_p. 假定信道慢变场景下有 $T_c \geqslant N_1 T_p$, 设计方案如下.

在一个相干时间 T_c 内, 对于由 N 个辐射单元构成的 RIS 天线, 前 N_1 个单元用于波束赋形, 其余 $N-N_1$ 个单元用于随机波束. 记从 Bob 到 Alice 端每个 RIS 单元信道信息为 h_n. 为实现波束赋形, 需预先估计前 N_1 个单元的信道信息. 由于所有辐射单元级联至一个基带通道, h_n 难以直接获得. 考虑 RIS 相移捷变速率可达微秒级 [21], 采用捷变 N_1+1 轮前 N_1 个单元的相移, 其余 $N-N_1$ 个单元相移保持不变的策略, 构造可逆矩阵, 反解出信道信息. 具体可用如下式子表示:

$$
(N_1+1)\begin{cases}
h_1 \mathrm{e}^{\mathrm{j}\theta_{1,1}} + h_2 \mathrm{e}^{\mathrm{j}\theta_{2,1}} + \cdots + h_{N_1} \mathrm{e}^{\mathrm{j}\theta_{N_1,1}} + \sum\limits_{n=N_1+1}^{N} h_n = \widehat{h}_{\mathrm{ba},1}, \\
h_1 \mathrm{e}^{\mathrm{j}\theta_{1,2}} + h_2 \mathrm{e}^{\mathrm{j}\theta_{2,2}} + \cdots + h_{N_1} \mathrm{e}^{\mathrm{j}\theta_{N_1,2}} + \sum\limits_{n=N_1+1}^{N} h_n = \widehat{h}_{\mathrm{ba},2}, \\
\qquad\qquad \vdots \\
h_1 \mathrm{e}^{\mathrm{j}\theta_{1,N_1}} + h_2 \mathrm{e}^{\mathrm{j}\theta_{2,N_1}} + \cdots + h_{N_1} \mathrm{e}^{\mathrm{j}\theta_{N_1,N_1}} + \sum\limits_{n=N_1+1}^{N} h_n = \widehat{h}_{\mathrm{ba},N_1}, \\
h_1 \mathrm{e}^{\mathrm{j}\theta_{1,N_1+1}} + h_2 \mathrm{e}^{\mathrm{j}\theta_{2,N_1+1}} + \cdots + + h_{N_1} \mathrm{e}^{\mathrm{j}\theta_{N_1,N_1+1}} + \sum\limits_{n=N_1+1}^{N} h_n = \widehat{h}_{\mathrm{ba},N_1+1},
\end{cases} \tag{18}
$$

其中, $\theta_{n,k}$ 表示第 k 轮捷变中第 n 个单元的相移, $\widehat{h}_{\mathrm{ba},k}$ 表示第 k 轮捷变后 Alice 基带侧探测的信道信息.

记

$$\boldsymbol{h}=\left[h_1,h_2,\ldots,h_{N_1},\sum_{n=N_1+1}^{N}h_n\right]^{\mathrm{T}},\quad \boldsymbol{A}=\begin{bmatrix} \mathrm{e}^{\mathrm{j}\theta_{1,1}} & \mathrm{e}^{\mathrm{j}\theta_{2,1}} & \cdots & \mathrm{e}^{\mathrm{j}\theta_{N_1,1}} & 1\\ \mathrm{e}^{\mathrm{j}\theta_{1,2}} & \mathrm{e}^{\mathrm{j}\theta_{2,2}} & \ddots & \mathrm{e}^{\mathrm{j}\theta_{N_1,2}} & 1\\ \vdots & \vdots & \ddots & \vdots & 1\\ \vdots & \vdots & \ddots & \vdots & 1\\ \vdots & \vdots & \ddots & \mathrm{e}^{\mathrm{j}\theta_{N_1,N_1}} & 1\\ \mathrm{e}^{\mathrm{j}\theta_{1,N_1+1}} & \mathrm{e}^{\mathrm{j}\theta_{2,N_1+1}} & \cdots & \mathrm{e}^{\mathrm{j}\theta_{N_1,N_1+1}} & 1 \end{bmatrix},$$

$$\widehat{\boldsymbol{h}}_{\mathrm{ba}}=[\widehat{h}_{\mathrm{ba},1},\widehat{h}_{\mathrm{ba},2},\ldots,\widehat{h}_{\mathrm{ba},N_1},\widehat{h}_{\mathrm{ba},N_1+1}]^{\mathrm{T}},$$

则有矩阵形式

$$\boldsymbol{A}\boldsymbol{h}=\widehat{\boldsymbol{h}}_{\mathrm{ba}}. \tag{19}$$

若矩阵 $\boldsymbol{A}$ 可逆, 则有

$$\boldsymbol{h}=\boldsymbol{A}^{-1}\widehat{\boldsymbol{h}}_{\mathrm{ba}}, \tag{20}$$

即可得所需的 $\boldsymbol{h}$.

问题转化为如何设计可逆矩阵 $\boldsymbol{A}$. 相移由 Alice 端自行配置, 因而可事先计算并存储可逆矩阵, 构造出 $\boldsymbol{A}$. 同时为了保证不因预设矩阵造成信息泄露, 可存储多组矩阵序列, 随机选取矩阵 $\boldsymbol{A}$ 用于信道估计. 此时, 对于 Alice 和 Bob 来说, 其探测的信道 $\widehat{\boldsymbol{h}}_{\mathrm{ba}}$ 和 $\widehat{\boldsymbol{h}}_{\mathrm{ab}}$ 仍是快变的.

当估计出 $\boldsymbol{h}$ 后, 在后续时刻, 前 N_1 个单元的相移采用一定方案设计, 用于生成有利于 Bob 的定向波束, 其余 $N-N_1$ 个单元的相移类似 RIS-A 方案随机设置. 在此期间, Bob 端等效信道状态信息为

$$\widehat{h}_{\mathrm{ab}}=\sum_{n=1}^{N_1}h_n\mathrm{e}^{\mathrm{j}\theta_n}+\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n}. \tag{21}$$

则 Bob 端接收信噪比可以表示为

$$\mathrm{SNR}_{\mathrm{b}}=\frac{P\left|\sum_{n=1}^{N_1}h_n\mathrm{e}^{\mathrm{j}\theta_n}+\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n}\right|^2}{N\sigma_n^2}. \tag{22}$$

由于 $\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n}$ 中 $\{h_n,n\geqslant N_1+1\}$ 未知且 $\{\theta_n,n\geqslant N_1+1\}$ 随机生成, 我们的策略为设计相移 $\{\theta_n,1\leqslant n\leqslant N_1\}$ 使得 $|\sum_{n=1}^{N_1}h_n\mathrm{e}^{\mathrm{j}\theta_n}|$ 最大. 为保证其最大, 由三角不等式, 只需使得相移对齐即可, 即

$$\sum_{n=1}^{N_1}h_n\mathrm{e}^{\mathrm{j}\theta_n}=\sum_{n=1}^{N_1}|h_n|. \tag{23}$$

易推得 $\theta_n=-\arg(h_n)$.

在该相干时间后续时间内, 均按照该策略进行波束赋形和密钥生成.

系统整体流程可归纳为 4 个阶段, 如图 6 所示.

(1) 通信准备阶段. 根据信道环境, 预估相干时间, 设计用于波束赋形的单元数 N_1.

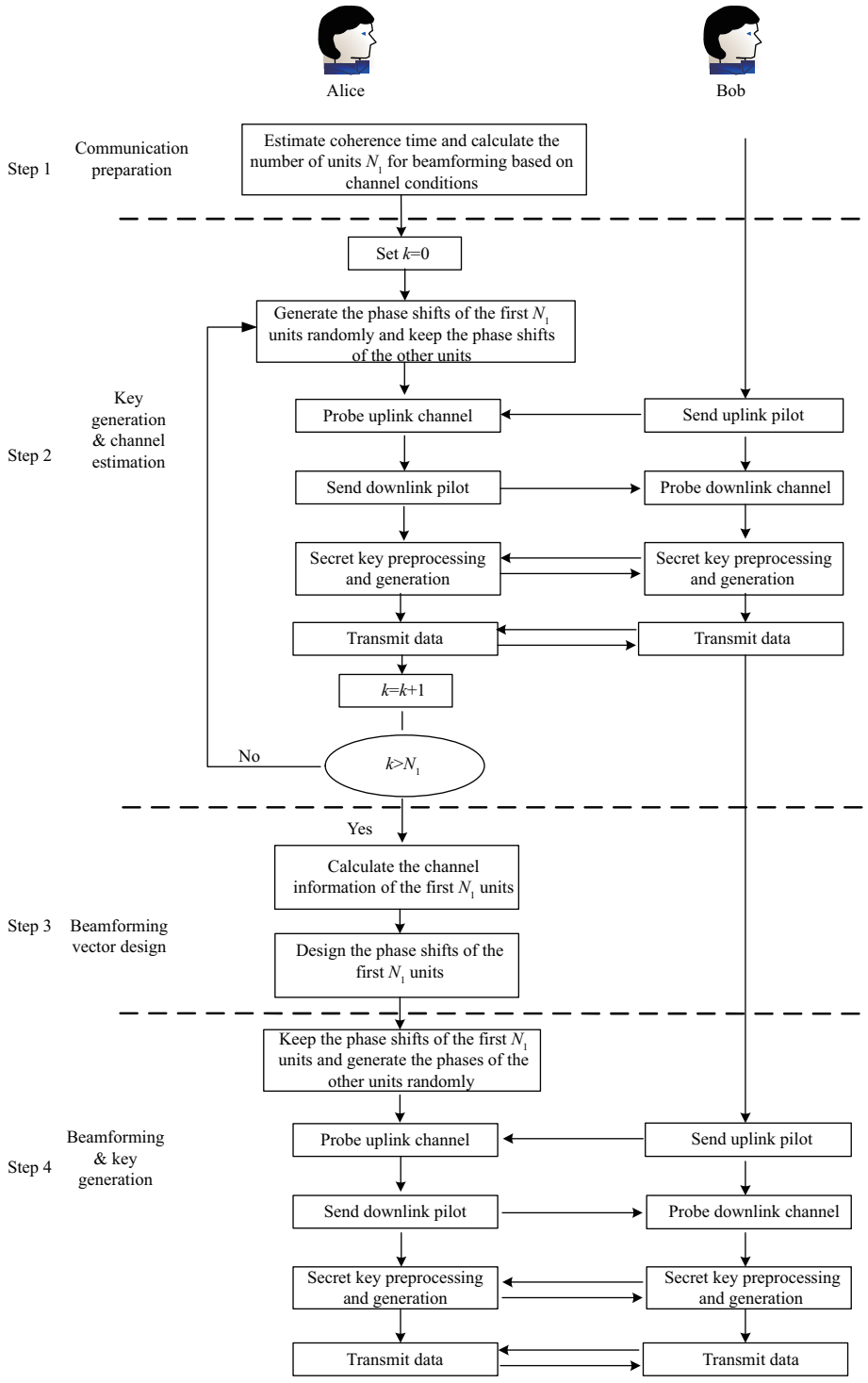

图 6 (网络版彩图) 基于 RIS 天线通信安全联合设计方案流程图

Figure 6 (Color online) The flow chart of communication and security integrated scheme based on RIS antenna

(2) 波束赋形前密钥生成及通信阶段. 初始设置计数器 $k = 0$, 然后执行 $(N_1 + 1)$ 轮相移捷变, 每

轮过程分为 4 个步骤.

(i) 相移设置: 随机生成前 N_1 个单元相移, 其余 $N-N_1$ 个单元相移保持不变;

(ii) 信道探测: 在相移配置完成的基础上, 同第 2 节, Alice 和 Bob 互发导频, 探测估计信道;

(iii) 密钥预处理及生成: 与第 2 节类似, 经过量化、信息协商、隐私放大后双方生成一致的密钥;

(iv) 数据传输: 通信双方利用生成的密钥加密传输信息.

(3) 波束赋形设计阶段. 根据第 3 步探测得到的信道, 利用式 (18)~(20) 计算前 N_1 个通道的 h_n, 然后利用式 (23) 设计最优相移, 用于波束赋形.

(4) 波束赋形后密钥生成及通信阶段. 此过程包含 4 个步骤.

(i) 相移设置: 固定保持前 N_1 个相位, 随机生成其余 $N-N_1$ 个相位;

(ii) 信道探测: 在相移配置完成的基础上, Alice 和 Bob 探测估计信道;

(iii) 密钥预处理及生成: 与第 2 节类似, 经过量化、信息协商、隐私放大后双方生成一致的密钥;

(iv) 数据传输: 通信双方利用生成的密钥加密传输信息, 并通过波束赋形增强双方通信质量.

从上述流程可以看到, 密钥生成及通信在整个过程持续进行, 对现有通信协议改动较小, 相较于 RIS-A 方案, 仅需增加额外的信道矩阵求解运算. 由于可以预先存储逆矩阵, 带来计算延迟和开销较小. 与 RIS-A 方案一样, 只需对中心节点设备进行改造. 需要说明的是, 当相干时间难以准确估计时, 可设置较小的 N_1 来保证系统的稳定性.

3.2 方案性能分析

3.2.1 通信性能分析

接下来, 从理论上分析该方案对通信性能的增量. 我们用平均信噪比 (average signal to noise ratio, ASNR) 来刻画通信性能. 首先从窃听者 Eve 来说, 平均接收信噪比表示为

$$\mathrm{ASNR_e}=\frac{\mathbb{E}(P|\sum_{n=1}^{N}h_{\mathrm{ae},n}\mathrm{e}^{\mathrm{j}\theta_n}|^2)}{N\sigma_n^2}=\frac{\mathbb{E}(P|\sum_{n=1}^{N_1}h_{\mathrm{ae},n}\mathrm{e}^{\mathrm{j}\theta_n}+\sum_{n=N_1+1}^{N}h_{\mathrm{ae},n}\mathrm{e}^{\mathrm{j}\theta_n}|^2)}{N\sigma_n^2}\overset{\text{(a)}}{=}\frac{P\sigma_{\mathrm{e}}^2}{\sigma_n^2}. \tag{24}$$

等式 (a) 成立由于 $h_{\mathrm{ae},n}$ 与 h_n 独立, 相应地, $\sum_{n=1}^{N_1}h_{\mathrm{ae},n}\mathrm{e}^{\mathrm{j}\theta_n}+\sum_{n=N_1+1}^{N}h_{\mathrm{ae},n}\mathrm{e}^{\mathrm{j}\theta_n}$ 仍然服从高斯分布. 易知所提方案并不会改变窃听性能.

对于 Bob 来说, 平均信噪比表示为

$$\mathrm{ASNR_b}=\frac{\mathbb{E}(P|\sum_{n=1}^{N_1}h_n\mathrm{e}^{\mathrm{j}\theta_n}+\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n}|^2)}{N\sigma_n^2}=\frac{\mathbb{E}(P|X_0+X_1+jY_1|^2)}{N\sigma_n^2}, \tag{25}$$

其中, $X_0=\sum_{n=1}^{N_1}|h_n|$, $X_1=\mathrm{Re}(\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n})$, $Y_1=\mathrm{Im}(\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n})$. 利用中心极限定理可知, X_0 服从高斯分布, 均值为 $N_1\sqrt{\frac{\pi}{4}}\sigma_{\mathrm{ab}}$, 方差为 $\frac{N_1(4-\pi)}{4}\sigma_{\mathrm{ab}}^2$; X_1 和 Y_1 服从高斯分布, 均值为 0, 方差为 $\frac{(N-N_1)\sigma_{\mathrm{ab}}^2}{2}$. 利用高斯分布的性质, 可推得

$$\mathbb{E}\left(|X_0+X_1+\mathrm{j}Y_1|^2\right)=\mathbb{E}\left((X_0+X_1)^2+Y_1^2\right)=\frac{N_1^2\pi+N_1(4-\pi)}{4}\sigma_{\mathrm{ab}}^2+(N-N_1)\sigma_{\mathrm{ab}}^2. \tag{26}$$

进一步可得

$$A\mathrm{SNR_b}=\left(1+\frac{N_1^2-N_1}{4N}\pi\right)\frac{P\sigma_{\mathrm{ab}}^2}{\sigma_n^2}. \tag{27}$$

由式 (27) 知, 相较于没有 RIS 的情况, Bob 的信噪比得到提升.

3.2.2 密钥容量分析

在 RIS 联合方案流程中, 考虑步骤 4 占比时间长, 主要分析该阶段性能, 即前 N_1 个单元相位固定, 其余 $N-N_1$ 个单元随机后的密钥性能. 此时 Bob 端探测的信道信息表示为

$$\widehat{h}_{\mathrm{ab}}=\sum_{n=1}^{N_1}|h_n|+\sum_{n=N_1+1}^{N}h_n\mathrm{e}^{\mathrm{j}\theta_n}. \tag{28}$$

可以看到, 式 (28) 中 $|h_n|$ 和 $h_n\mathrm{e}^{\mathrm{j}\theta_n}$ 分布不一致, $\widehat{h}_{\mathrm{ab}}$ 分布难以保证为高斯分布, 即相较于 RIS-A 方案密钥容量会有损失, 闭式解也难以获得. 这里, 考虑极端情况, 即在信道不变下, 可知 $\widehat{h}_{\mathrm{ab},I}$ 服从高斯分布, 均值为 $\sum_{n=1}^{N_1}|h_n|$, 方差为 $(N-N_1)\sigma_{\mathrm{ab}}^2$. 相应地, 可得 $\rho(\widehat{h}_{\mathrm{ab},I},\widehat{h}_{\mathrm{ba},I})=\frac{1}{1+\eta'_{\mathrm{ab}}}$, $\eta'_{\mathrm{ab}}=\frac{N\sigma_n^2}{P\sigma_{\mathrm{ab}}^2 l_p(N-N_1)}$. 则可获得密钥容量的下界 $C_{\mathrm{SK\_lower}}$ 为

$$C_{\mathrm{SK\_lower}}=\frac{1}{2}\log_2\left(\frac{1+\eta'_{\mathrm{ab}}}{1+\eta'_{\mathrm{ab}}-\frac{1}{1+\eta'_{\mathrm{ab}}}}\right). \tag{29}$$

可以看到, N_1/N 的比例影响密钥容量下界. N_1/N 越大, 越少的单元用于密钥生成, 相应地, 容量降低, 反之亦然.

同样的密钥容量上界为快变环境下的密钥容量, 即为

$$C_{\mathrm{SK\_upper}}=-\frac{1}{2}\log_2\left(1-\left(\frac{\sigma_{\mathrm{ab}}^2}{\sigma_{\mathrm{ab}}^2+\sigma_n^2/(Pl_p)}\right)^2\right). \tag{30}$$

3.3 资源分配问题及求解

由式 (27), (29), (30) 知, 密钥容量和平均信噪比与发送功率 P、RIS 单元数量 N 和赋形单元数量 N_1 等参数相关. N_1 越大, 平均信噪比越强, 密钥容量越低, 反之亦然, 即参数选取存在折中. 基于此, 构造优化问题为, 以最小化发送功率为目标, 在给定 RIS 单元数量以及满足系统安全与通信指标的情况下, 设计最优的 N_1. 优化问题表述如下:

$$\min_{N_1}\ P, \tag{31a}$$

$$\text{s.t. } C_{\mathrm{SK\_lower}}\geqslant\zeta_{\mathrm{sk}}, \tag{31b}$$

$$A\mathrm{SNR}_{\mathrm{b}}\geqslant\gamma_{\mathrm{b}}, \tag{31c}$$

$$N_1T_p\leqslant T_c, \tag{31d}$$

$$N_1\leqslant N, \tag{31e}$$

其中, ζ_{sk} 表示密钥容量门限, γ_{b} 表示信噪比门限.

代入式 (27) 和 (29), 可得

$$\min_{N_1}\ P, \tag{32a}$$

$$\text{s.t. } P\geqslant\frac{(\sqrt{2^{\zeta_{\mathrm{sk}}}(2^{\zeta_{\mathrm{sk}}}-1)}+(2^{\zeta_{\mathrm{sk}}}-1))N\sigma_n^2}{\sigma_{\mathrm{ab}}^2 l_p(N-N_1)}, \tag{32b}$$

$$P\geqslant\frac{4N\gamma_{\mathrm{b}}\sigma_n^2}{\sigma_{\mathrm{ab}}^2((N_1^2-N_1)\pi+4N)}, \tag{32c}$$

$$N_1\leqslant N_{\min},\ \ N_{\min}=\min(T_c/T_p,N). \tag{32d}$$

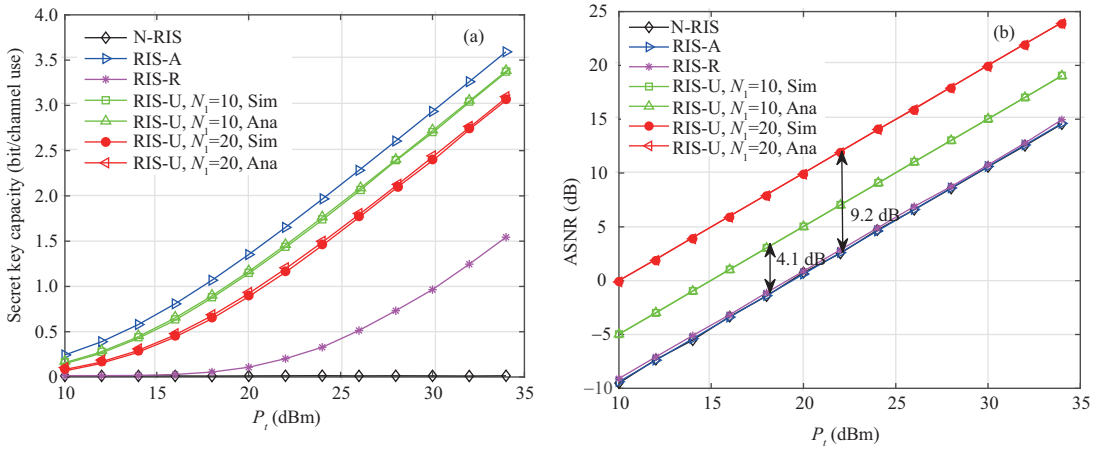

图 7 (网络版彩图) 不同发送功率下, (a) 密钥容量 ($N = 40$) 和 (b) 通信性能 ($N = 40$)

Figure 7 (Color online) Secret key capacity (a) and communication performance (b) versus transmit power ($N = 40$)

进一步引入函数 $f(N_1)$ 和 $g(N_1)$, 并定义为

$$f(N_1) = \frac{(\sqrt{2^{\zeta_{\rm sk}}(2^{\zeta_{\rm sk}}-1)} + (2^{\zeta_{\rm sk}}-1))N\sigma_n^2}{\sigma_{\rm ab}^2 l_p (N - N_1)}, \tag{33}$$

$$g(N_1) = \frac{4N\gamma_{\rm b}\sigma_n^2}{\sigma_{\rm ab}^2((N_1^2 - N_1)\pi + 4N)}. \tag{34}$$

易知 $f(N_1)$ 关于 N_1 递增, $g(N_1)$ 关于 N_1 递减, 则有 $f(1) \leqslant f(N_1) \leqslant f(N_{\min})$, $g(N_{\min}) \leqslant g(N_1) \leqslant g(1)$. 为求解最优 N_1, 分 3 种情况讨论.

(1) 若 $f(N_{\min}) \leqslant g(N_{\min})$, 则曲线 $f(N_1)$ 和 $g(N_1)$ 没有交点, 易知系统所需最小功率 $P_{\min} = g(N_{\min})$, 最优 $N_1^* = N_{\min}$.

(2) 若 $f(1) \geqslant g(1)$, 则曲线 $f(N_1)$ 和 $g(N_1)$ 没有交点, 易知系统所需最小功率 $P_{\min} = f(1)$, 最优 $N_1^* = 1$.

(3) 若 $f(1) \leqslant g(1), f(N_{\min}) \geqslant g(N_{\min})$, 则曲线 $f(N_1)$ 和 $g(N_1)$ 有且仅有一个交点. 系统所需最小功率即为交点 $P_{\min} = f(N_1^\circ) = g(N_1^\circ)$. 由于最优点 N_1° 不一定为整数, 记 $N_1^\times$ 表示 N_1° 向下取整值, 然后分两种情况讨论:

若 $g(N_1^\times) \leqslant f(N_1^\times + 1)$, 则所需最小功率 $P_{\min} = g(N_1^\times)$, 最优 $N_1^* = N_1^\times$;

若 $g(N_1^\times) \geqslant f(N_1^\times + 1)$, 则所需最小功率 $P_{\min} = f(N_1^\times + 1)$, 最优 $N_1^* = N_1^\times + 1$.

至此, 可得参数的最优配置策略.

3.4 方案仿真验证

为验证理论分析结果, 本小节利用 ITE 工具箱计算互信息量并进行蒙特卡罗仿真实验, 参数配置同 2.3 小节, 并与 RIS-R, RIS-A 以及 N-RIS 方案的性能进行对比.

图 7(a) 给出了信道环境不变时不同发送功率下不同 N_1 的密钥性能. 可以看到, RIS-U 方案的理论解与仿真值一致. 在没有引入 RIS 的情况下, 密钥容量逼近于 0; 而引入 RIS 后, 随着发送功率的提高, 密钥容量均显著提升. 同等条件下, RIS-A 方案性能最好, 而由于 RIS-U 方案中部分辐射单元的相

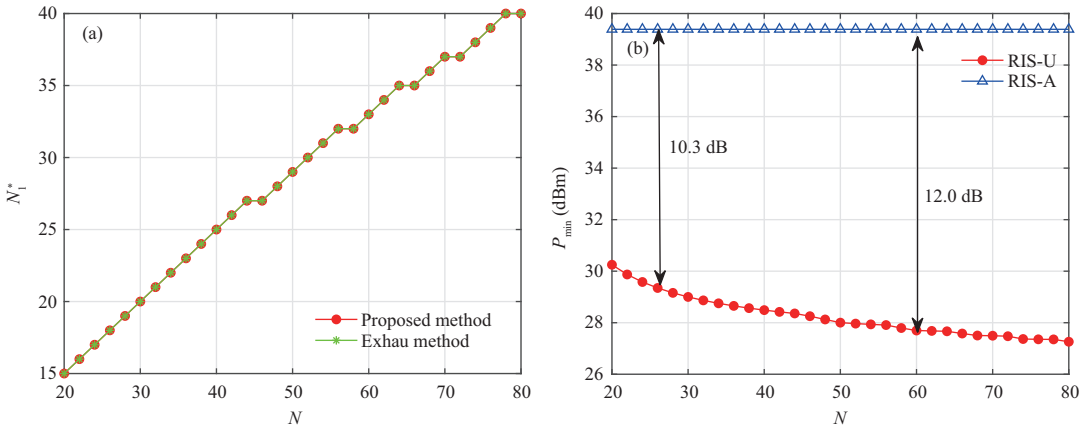

图 8 (网络版彩图) 联合方案性能. (a) 不同 N 下满足 QoS 所需最优 N_1^*; (b) 不同 N 下满足 QoS 所需最小功率 $P_{\min}$

Figure 8 (Color online) Communication and security integrated scheme performance. (a) The optimal N_1^* versus N under QoS; (b) the minimum power $P_{\min}$ versus N under QoS

移设置为定值, 因而 RIS-U 方案密钥容量次之. 随着 N_1 的增加, 更多单元用于波束赋形, RIS-U 方案密钥容量下降, 验证了理论分析结果.

图 7(b) 给出了信道环境不变时不同发送功率不同 N_1 下 Bob 端的平均信噪比. 可以看到, 随着发送功率的提高, 平均信噪比提升, 且与理论值一致. N-RIS 和 RIS-A 方案通信性能一致, 这是因为 RIS-A 方案对子信道随机相位加权合并后, 等效的随机波束与原信道统计特性一致, 即采用 RIS-A 方案不会带来通信性能损失. 而 RIS-R 方案通信性能比 RIS-A 方案略高, 这是因为 RIS 作为反射面部署在环境中引入反射路径, 可以提高接收信噪比, 然而由于级联路径损耗与反射路径距离乘积成正比, 若反射系数不精心配置, 性能增益很小 [21]. 采用 RIS-U 方案后, 信噪比显著提升, 相较于 RIS-A 方案, $N_1 = 10$ 时, 信噪比提升 4.1 dB, $N_1 = 20$ 时, 信噪比提升 9.2 dB. 比较图 7(a) 和 (b), 相较 N-RIS 方案, RIS-U 方案对密钥性能和通信性能均带来提升. 而增大 N_1, 密钥性能下降, 通信性能提升, 反之亦然, 即存在一个折中, 需要进行最优参数配置.

图 8 给出了在给定 QoS 指标和 N 的情况下, 采用本文算法获得的最优 N_1^* 以及最小发射功率 $P_{\min}$, 并与穷举搜索算法 (记为 Exhau) 性能进行对比. 参数设置为 $\zeta_{\text{sk}} = 4$ bit/channel use, $T_c = 50$ ms, $\gamma_{\text{b}} = 20$ dB. 从图 8(a) 中可以看到, 本文给出算法与穷举搜索算法性能一致, 验证了算法有效性. 从图 8(b) 中可以看到, 在满足 QoS 指标约束下, 相较于第 2 节提出的 RIS-A 方案, 通过设计最优的 N_1^*, RIS-U 方案可显著降低发射功率, 当 $N = 60$ 时, 所需功率下降 12 dB, 随着 N 的增加, 功率可进一步降低. 当然辐射单元数量的增加还需考虑终端的尺寸等因素, 后续可进一步结合实现复杂度等约束条件进行参数设计.

4 结论

本文利用 RIS 对电磁波的快速、灵活调控能力, 提出了 RIS 天线辅助的物理层密钥生成方案, 可使静态场景下密钥容量达到与快变环境下同等性能, 且对现有设备改动很小. 进一步, 提出了通信安全联合设计方案, 给出最优参数配置策略, 可在保证密钥容量和通信性能的基础上, 降低发射功率, 有

效满足未来低功耗物联网场景安全通信需求. 基于 RIS 原型机的密钥生成验证平台有待后续进一步研究.

参考文献

1 You X H, Wang C-X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301

2 Zhang J, Duong T Q, Marshall A, et al. Key generation from wireless channels: a review. IEEE Access, 2016, 4: 614–626

3 Xiao S F, Guo Y F, Huang K, et al. High-rate secret key generation aided by multiple relays for Internet of Things. Electron Lett, 2017, 53: 1198–1200

4 Jin L, Zhang S J, Lou Y, et al. Secret key generation with cross multiplication of two-way random signals. IEEE Access, 2019, 7: 113065

5 Aldaghri N, Mahdavifar H. Physical layer secret key generation in static environments. IEEE Trans Inform Forensic Secur, 2020, 15: 2692–2705

6 Zhao Y J, Yu G H, Xu H Q. 6G mobile communication networks: vision, challenges, and key technologies. Sci Sin Inform, 2019, 49: 963–987 [赵亚军, 郁光辉, 徐汉青. 6G 移动通信网络: 愿景, 挑战与关键技术. 中国科学: 信息科学, 2019, 49: 963–987]

7 Ji Z J, Yeoh P L, Zhang D, et al. Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans Veh Technol, 2021, 70: 1030–1034

8 Hu X Y, Jin L, Huang K, et al. Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment. IEEE Wireless Commun Lett, 2021, 10: 1867–1870

9 Staat P, Elders-Boll H, Heinrichs M, et al. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In: Proceedings of IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2021. 745–751

10 Shlezinger N, Alexandropoulos G C, Imani M F, et al. Dynamic metasurface antennas for 6G extreme massive MIMO communications. IEEE Wireless Commun, 2021, 28: 106–113

11 Shlezinger N, Dicker O, Eldar Y C, et al. Dynamic metasurface antennas for uplink massive MIMO systems. IEEE Trans Commun, 2019, 67: 6829–6843

12 Lu Y, Dai L L. Reconfigurable intelligent surface based hybrid precoding for THz communications. 2020. ArXiv:2012.06261

13 Zhang J, Rajendran S, Sun Z, et al. Physical layer security for the Internet of Things: authentication and key generation. IEEE Wireless Commun, 2019, 26: 92–98

14 Ruotsalainen H, Zhang J Q, Grebeniuk S. Experimental investigation on wireless key generation for low-power wide-area networks. IEEE Internet Things J, 2020, 7: 1745–1755

15 Madiseh M G, Neville S W, McGuire M L. Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation. IEEE Trans Inform Forensic Secur, 2012, 7: 1278–1287

16 Yang L, Yang J X, Xie W W, et al. Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans Veh Technol, 2020, 69: 12296–12300

17 Zhang J Q, He B, Duong T Q, et al. On the key generation from correlated wireless channels. IEEE Commun Lett, 2017, 21: 961–964

18 Chen D J, Qin Z, Qin Z G, et al. On the security of fast secret key generation protocol with virtual channel approach. J Univ Electr Sci Tech China, 2015, 1: 112–116 [陈大江, 秦臻, 秦志光, 等. 基于虚拟信道的快速密钥生成协议的安全性分析. 电子科技大学学报, 2015, 1: 112–116]

19 Li G Y, Hu A Q, Zhang J Q, et al. Security analysis of a novel artificial randomness approach for fast key generation. In: Proceedings of IEEE Global Communications Conference, 2017. 1–6

20 Guan X R, Wu Q Q, Zhang R. Intelligent reflecting surface assisted secrecy communication: is artificial noise helpful or not? IEEE Wireless Commun Lett, 2020, 9: 778–782

21 Wu Q Q, Zhang S W, Zheng B X, et al. Intelligent reflecting surface-aided wireless communications: a tutorial. IEEE Trans Commun, 2021, 69: 3313–3351

Secret key generation scheme based on RIS antenna for static environments

Jie YANG[1,2], Xinsheng JI[1,2*], Kaizhi HUANG[1,2], Jianlei ZHAO[2] & Xinrong GUAN[3]

1. *National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002*, China*;
2. *Purple Mountain Laboratories: Networking, Communications and Security, Nanjing* 211189*, China*;
3. *College of Communication Engineering, Army Engineering University of PLA, Nanjing* 210007*, China*
* Corresponding author. E-mail: jxs_ndsc@126.com

Abstract A conventional secret key generation scheme achieves a low secret key rate in static environments. To solve this problem, the reconfigurable intelligent surface (RIS) antenna is merged with the device at the base station and is firstly proposed for secret key generation. By tuning the phase shifts at the RIS, a random varying beam can be generated and combined with the original wireless channel to form a new equivalent channel so that the key capacity is not subject to the time variance of the wireless channel. Then the closed-form solution is derived. Theoretical analysis and simulation show that the performance can be increased to that of a fast varying channel with limited radiating units. Moreover, the proposed scheme is superior to the existing schemes, in which the RIS is used as a reflective surface, over performance gain and preventing information disclosure. To further develop the gain of RIS, a joint design scheme is proposed, where some units are used for key generation, and some units are used for beamforming. Finally, the joint's closed-form solution scheme is derived. Finally, on the basis of satisfying the key capacity and communication performance, an optimal resource allocation strategy is proposed. Simulation results illustrate that the key capacity and communication performance can be improved simultaneously.

Keywords reconfigurable intelligent surface, secret key generation, physical layer security, static environment, resource allocation