

准静态场景下基于智能超表面的密钥生成方法

郝一诺, 金梁, 黄开枝, 肖帅芳

(信息工程大学, 河南 郑州 450001)

摘要: 针对物联网准静态场景中信道变化缓慢、密钥速率低的问题, 提出了一种基于智能超表面 (RIS, reconfigurable intelligent surface) 的密钥生成方法。首先, 利用 RIS 的捷变特性构造快速变化的信道; 然后, 基站 (BS, base station) 与合法用户通过信道估计、量化、信息协商等步骤从信道信息中提取对称密钥; 最后, 对相干时间内密钥生成和数据传输进行最优时间分配, 实现最大传输速率的“一次一密”。仿真结果表明, 所提方法的密钥速率高于现有的中继辅助、随机信号流和随机数方法, 并且随着 RIS 反射单元个数和相干时间内信道估计次数的增加, 密钥速率有进一步的提高。

关键词: 物理层安全; 密钥生成; 智能超表面; 准静态场景

中图分类号: TN918.82

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021027

Key generation method based on reconfigurable intelligent surface in quasi-static scene

HAO Yinuo, JIN Liang, HUANG Kaizhi, XIAO Shuaifang

Information Engineering University, Zhengzhou 450001, China

Abstract: Aiming at the problems of slow channel changes and low key generation rate in IoT quasi-static scenarios, a key generation method based on reconfigurable intelligent surface (RIS) was proposed. First, the agility characteristics of RIS was used to construct a fast-changing channel. Then, the base station and legitimate users extracted a consistent key from the channel information through channel estimation, conversion, and information negotiation. Finally, optimal time allocation for data transmission and key generation in the coherent time to achieve the maximum transmission rate of one-time pad. The simulation results show that the key generation rate of proposed method is higher than that of the existing relay-assisted method, random signal flow method and random number method, and as the number of RIS reflection units and frequency of channel estimation in the coherence time increase, the key generation rate will be further improve.

Keywords: physical layer security, key generation, reconfigurable intelligent surface, quasi-static scene

收稿日期: 2020-11-16; 修回日期: 2021-01-11

通信作者: 金梁, liangjin@236.net

基金项目: 国防科技创新特区; 国家自然科学基金 (61871404)

Foundation Items: National Defense Technology Innovation Special Zone, The National Natural Science Foundation of China (61871404)

论文引用格式: 郝一诺, 金梁, 黄开枝, 等. 准静态场景下基于智能超表面的密钥生成方法[J]. 网络与信息安全学报, 2021, 7(2): 77-85.

HAO Y N, JIN L, HUANG K Z, et al. Key generation method based on reconfigurable intelligent surface in quasi-static scene [J]. Chinese Journal of Network and Information Security, 2021, 7(2): 77-85.

1 引言

物理层密钥生成技术以信道状态信息 (CSI, channel state information) 作为密钥源, 密钥更新速度依赖于 CSI 的快速变化。然而, 在智能家居、环境监测等典型的物联网场景中, 信道变化往往十分缓慢, 这类通信节点和物理环境均固定不变的信道被定义为准静态信道^[1]。在准静态场景中, 多径相位不变、节点不移动导致多普勒效应不明显、密钥源的随机性差、密钥更新缓慢, 严重制约了密钥速率。要解决准静态场景下密钥速率低的问题, 其本质在于提高密钥源的随机性。

目前, 针对准静态场景中提高密钥速率的研究已经取得了一些进展, 主要分为以下 3 类。

①借助频域、空域等多维资源提高密钥源的随机性。例如, 文献[2]提出了多入多出 (MIMO, multiple-in multiple-out) 场景下, 利用随机波束成形对信道进行随机加权处理的密钥生成方法, 利用空域资源提高密钥源的随机性; 文献[3]参照频率跳变表改变多径信道的频率, 并使用多个信道的 CSI 平均值进行密钥生成, 利用频率资源提高密钥源的随机性。但是, 这类方法需要引入丰富的空频域资源, 在资源受限的环境中难以实现^[4]。②利用人工随机源发射随机信号, 通过接收信号的随机性提高密钥源的随机性。例如, 文献[5]提出了一种基于人工随机源生成密钥的方法; 文献[6]利用 MIMO 接收信号进行人工随机源设计, 提高了密钥速率。但是, 这类方法没有从本质上改变信道的随机性, 并且恒定的信道参数会导致窃听者易于预测人工信号, 因此该方法的密钥速率仍然受到限制^[7]。③利用中继协作辅助密钥生成, 通过增加互易信道个数提高密钥源的随机性。例如, 文献[8]研究了双向中继系统中密钥生成的问题, 提出了 4 种基于放大转发的密钥生成方案; 文献[9]在文献[8]的基础上, 研究了多径环境下基于相对幅度和相对相位的密钥生成方案; 文献[4]基于中继节点辅助和安全网络编码, 将中继节点与合法通信双方之间的信道引入密钥源, 提高了密钥源的随机性。但是, 这类方法同样没有提高信道随机性, 并且需要设立中继进行辅助信息的分发等, 因此该方法的密钥源的随机性有限, 并且在实际应用

中存在局限性。综上所述, 在准静态场景中以低成本快速更新密钥仍然是一个有待解决的问题。

近年来, 随着射频微机电系统 (RFMEMS, radio frequency micro-electro-mechanical system) 的快速发展和可编程可重构超表面的广泛应用, 智能超表面 (RIS, reconfigurable intelligent surface) 作为一种低功耗、高效率的数据通信技术, 被越来越多地应用于无线数据传输中。其中, RIS 基于电磁材料, 由无源阵列结构组成, 该结构中存在数百个反射单元, 能够对多径信号进行反射、散射和透射, 并且以低功耗连续或离散地调整每个反射信号的相位^[10]。RIS 上每个反射信号相位信息的改变最快可以在 $1\ \mu\text{s}$ 内完成^[11], 这使利用 RIS 构建低成本的动态信道具有可行性。因此, 利用 RIS 定制无线传输环境以获得物理层安全增益的方法越来越多地被提出^[12]。

然而, 目前提出的基于 RIS 的物理层安全方法主要利用 RIS 的可编程特性, 集中于对 RIS 反射系数和预编码矩阵进行波束成形的联合设计, 通过增加接收功率的方法实现安全传输^[12-15]。事实上, 利用 RIS 的快速捷变性以及实时可重构性定制信道环境, 可以通过人为拓展电磁物理参数空间, 提高对电磁波传输性态的操控自由度, 对于物理层密钥生成技术具有更为重大的意义。具体而言, 将 RIS 用于密钥生成具有以下优势: ①利用 RIS 的快速捷变性和实时可重构特性, 可以人为控制多径信号的相移, 定制快速变化的信道环境, 从本质上提高密钥源的随机性; ②RIS 仅对信号进行无源的反射、散射和透射, 因此功耗低且不引入额外的信号干扰; ③RIS 易于广泛部署在已有建筑物表面, 成本较低、实用性高。因此, 利用 RIS 提供动态实时可重构的无线环境, 从而在根本上扩大物理层密钥技术共享随机源的信息和随机性, 是一个具有深远意义和实用价值的研究方向。

基于以上分析, 本文提出了一种面向物联网准静态场景的基于 RIS 的密钥生成方法。首先, 利用 RIS 改变反射信号的相位信息构造快速变化的信道; 然后, 基站 (BS, base station) 与合法用户在相干时间内互发导频进行信道估计, 获得复合 CSI; 之后, 双方通过量化、信息协商、隐

私放大等步骤，从 CSI 中提取对称密钥；最后，根据 Shannon “完美保密” 的思想^[16]，对相干时间内的密钥生成和数据传输进行最优时间分配，达到最大传输速率的“一次一密”。仿真结果表明，该方法能够有效增加信道的随机性，从而提高密钥速率，并且通过时间最优化设计，提高“一次一密”速率。

2 系统模型

考虑准静态场景的信道特性，本文将信道建模为准静态块衰落模型，即在相干时间内 CSI 保持不变，在相干时间之间为衰落信道，CSI 发生变化。由于准静态特性，上述信道模型相干时间较长、信道变化缓慢，因此考虑在传统物联网通信模型中加入一个 RIS，构造基于 RIS 的密钥生成系统模型，通过不断改变反射信号的相位信息构造快速变化的信道。

基于 RIS 的密钥生成系统模型如图 1 所示，存在 BS、合法用户 k 、被动窃听者 (Eve) 以及 RIS。BS 与合法用户 k 之间在 TDD 模式下传输窄带信号，保证了信道的互易性。其中，BS 有 M 根天线，合法用户 k 和 Eve 均为单天线。RIS 有 N 个反射单元，RIS 控制器可以通过有线控制链路对 RIS 的反射单元进行编程，从而改变反射信号的相位信息。为了构造快变信道，RIS 上的控制器依据随机控制信号控制 RIS 上反射系数的快速变化，从而使每次信道估计所得 CSI 都与前一刻不同。

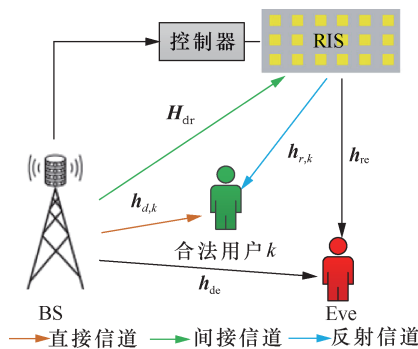


图 1 基于 RIS 的密钥生成系统模型
Figure 1 Key generation system model based on RIS

定义 $\mathbf{C}^{x \times y}$ 表示维度为 $x \times y$ 的矩阵。考虑如下 3 类信道：直接信道、间接信道和反射信道^[12]。其中，直接信道 $\mathbf{h}_{d,k} = [h_{d,k1}, h_{d,k2}, \dots, h_{d,kM}] \in \mathbf{C}^{1 \times M}$ 为 BS 与合法用户 k 之间的信道；间接信道 $\mathbf{H}_{dr} = [h_{dr,1},$

$h_{dr,2}, \dots, h_{dr,N}]^T \in \mathbf{C}^{N \times M}$ ， $\mathbf{h}_{dr,i} = [h_{dr,i,1}, h_{dr,i,2}, \dots, h_{dr,i,N}] \in \mathbf{C}^{1 \times M}$ 为 BS 与 RIS 之间的信道；反射信道 $\mathbf{h}_{r,k} = [h_{r,k1}, h_{r,k2}, \dots, h_{r,kN}] \in \mathbf{C}^{1 \times N}$ 为 RIS 与合法用户 k 之间的信道。由于 RIS 对于信号的反射、散射以及对于信号相位的快速改变， $\mathbf{H}_{dr}$ 和 $\mathbf{h}_{r,k}$ 建模为快速变化的小尺度衰落信道， $\mathbf{h}_{d,k}$ 建模为大尺度衰落信道。

根据电磁波的空间传播特性，不同信道之间具有独立性，上下行信道之间具有互易性。假设每种信道均服从均值为 0、方差为 σ^2 的高斯分布，且合法用户和 Eve 接收到的噪声均为独立同分布的高斯白噪声。

为了不暴露自身位置，Eve 只进行被动窃听，即只对信息进行窃听，不对信息传输过程进行干扰，不参与数据传输和密钥生成过程。由于 Eve 与合法用户之间的距离大于半个波长，信道之间互不相关，所以窃听者不能根据自身的 CSI 推测出合法用户的 CSI。

3 基于 RIS 的密钥生成方法

本节基于上述系统模型及典型点对点物理层密钥生成方法，设计了一种基于 RIS 的密钥生成方法。首先，RIS 进行多次反射系数的快速随机变化，构造高随机性的快变信道；然后，BS 和合法用户在相干时间内进行多次信道估计，并对获得的复合 CSI 进行量化、信息协商和隐私放大，生成对称密钥；最后，在相干时间内对密钥生成和数据传输进行最优时间分配，实现了最大传输速率的“一次一密”。

3.1 构造快变信道

与传统密钥生成模型不同，本文通过控制 RIS 的反射系数，快速随机改变 RIS 反射信号的相位信息，从而扩大 RIS 与合法用户之间信道的熵，构造快速变化的小尺度衰落信道。

如图 1 所示，定义 $\mathbf{h}_{b,k} \in \mathbf{C}^{1 \times M}$ 代表 BS 与合法用户 k 之间的复合信道，则有：

$$\begin{aligned} \mathbf{h}_{b,k} &= \mathbf{h}_{d,k} + \mathbf{h}_{r,k} \Theta \mathbf{H}_{dr} = \\ &= \mathbf{h}_{d,k} + \left[\sum_n h_{r,kn} e^{j\varphi_n} h_{dr,n,1}, \sum_n h_{r,kn} e^{j\varphi_n} h_{dr,n,2}, \dots, \right. \\ &\quad \left. \sum_n h_{r,kn} e^{j\varphi_n} h_{dr,n,M} \right] \end{aligned} \quad (1)$$

其中, $\Theta = \text{diag}(\theta) \in \mathbf{C}^{N \times N}$ 表示 RIS 的反射系数^[17], $\theta = [\theta_1, \theta_2, \dots, \theta_N]^T \in \mathbf{C}^{N \times 1}$, $\theta_n \in \Phi$ 。 Φ 表示第 $n(n \in \{1, 2, \dots, N\})$ 个反射单元的反射系数 θ_n 的取值范围。考虑 θ 连续变化的情况, 即

$$\Phi = \{\theta_n | \theta_n = e^{j\varphi_n}, \varphi_n \in [0, 2\pi)\} \quad (2)$$

因此, 通过快速改变 RIS 反射系数 θ 的取值, 可以极大程度地增强信道 $h_{b,k}$ 的 CSI 时变性, 提高密钥源的熵。

3.2 信道估计

在相干时间内, BS 与合法用户互发导频, 进行一次信道估计。同时, BS 控制 RIS 进行快速相位改变, 保证每次信道估计时 RIS 的反射系数都不同。由于准静态信道时变性差, 所以相干时间内可进行多次信道估计。

以第 $i(i \in \{1, 2, \dots, L\})$ 次信道估计为例, 令 θ_i 和 $h_{b,k,i}$ 分别表示第 i 次信道估计时 θ 和 $h_{b,k}$ 的值, $X_{b,k,i} \in \mathbf{C}^{M \times l}$ 和 $x_{k,b,i} \in \mathbf{C}^{l \times l}$ 分别表示第 i 次信道估计中 BS 向合法用户 k 以及合法用户 k 向 BS 发送的长度为 l 的导频信息。在信道估计阶段, 对 BS 端多天线信号进行等增益合并 (EGC, equal gain combining), 令 $y_{k,b,i} \in \mathbf{C}^{l \times l}$ 和 $Y_{b,k,i} \in \mathbf{C}^{l \times l}$ 分别表示合法用户 k 和 BS 接收到的信号, 从参考文献[18-19]可得:

$$y_{k,b,i} = (h_{d,k} + h_{r,k} \theta_i H_{\text{dr}}) X_{b,k,i} + n_{k,b,i} \quad (3)$$

$$Y_{b,k,i} = w (h_{d,k}^H + H_{\text{dr}}^H \theta_i h_{r,k}^H) x_{k,b,i} + n_{b,k,i} \quad (4)$$

其中, $w = [1, 1, \dots, 1] \in \mathbf{C}^{1 \times M}$ 为 EGC 向量, $n_{b,k,i}$ 和 $n_{k,b,i}$ 分别代表第 i 次信道估计时, BS 和合法用户 k 接收到的噪声。采用迫零算法, 令 $\tilde{h}_{k,b,i}$ 和 $\tilde{h}_{b,k,i}$ 分别表示合法用户 k 和 BS 对于信道 $h_{b,k,i}$ 的估计值, 则

$$\begin{aligned} \tilde{h}_{k,b,i} &= \frac{X_{b,k,i}^T}{\|X_{b,k,i}\|^2} y_{k,b,i} = \\ &= \frac{h_{d,k,i} + h_{r,k,i} \theta_i H_{\text{dr},i}}{\|X_{b,k,i}\|^2} x_{k,b,i} + \frac{X_{b,k,i}^T}{\|X_{b,k,i}\|^2} n_{k,b,i} \end{aligned} \quad (5)$$

$$\begin{aligned} \tilde{h}_{b,k,i} &= \frac{x_{k,b,i}^T}{\|x_{k,b,i}\|^2} Y_{b,k,i} = \\ &= \frac{w (h_{d,k,i}^H + H_{\text{dr},i}^H \theta_i h_{r,k,i}^H)}{\|x_{k,b,i}\|^2} x_{k,b,i} + \frac{x_{k,b,i}^T}{\|x_{k,b,i}\|^2} n_{b,k,i} \end{aligned} \quad (6)$$

经过 L 次信道估计, 令 $\tilde{H}_{b,k}$, $\tilde{H}_{k,b}$ 分别表示 BS 和合法用户 k 获得的总体信道估计值, 则

$$\tilde{H}_{b,k} = [\tilde{h}_{b,k,1}, \tilde{h}_{b,k,2}, \dots, \tilde{h}_{b,k,L}]^T \quad (7)$$

$$\tilde{H}_{k,b} = [\tilde{h}_{k,b,1}, \tilde{h}_{k,b,2}, \dots, \tilde{h}_{k,b,L}]^T \quad (8)$$

根据 2.1 节的分析可知, 间接信道 H_{dr} 和反射信道 $h_{r,k}$ 为小尺度衰落信道且快速变化, 因此本文所提方法将 BS 与合法用户 k 之间的复合信道 $h_{b,k}$ 作为共享随机源进行密钥生成, 该密钥源具有很高的随机性。

3.3 提取密钥

从共享随机源中提取密钥包含 3 个步骤, 即量化、信息协商和隐私放大。首先, BS 与合法用户 k 分别对 $\tilde{H}_{b,k}$ 和 $\tilde{H}_{k,b}$ 进行量化, 通过设置量化间隔将连续信号量化成离散信号, 生成初始密钥; 然后, 为了纠正或去除初始密钥中不一致的比特, BS 在信息协商步骤中根据 Cascade 协议^[20]对量化后的信号进行纠错编码, 生成协商信息 γ 并发送给合法用户 k , 合法用户 k 根据接收到的 γ 恢复出协商后的序列; 最后, 为了提高合法用户与窃听者间密钥的比特不一致率 (BMR, bit mismatch ratio), BS 和合法用户 k 在隐私放大步骤中使用 Hash 函数 SHA-256 对协商后的序列进行置换混淆和随机抽取^[21], 获得对称密钥。

3.4 “一次一密”最优化设计

相干时间内密钥生成与数据传输时隙分布如图 2 所示。在相干时间 T 内, 用于密钥生成的时间为 T_k , 用于数据传输的时间为 T_t , 每次信道估计所占时间为 T_l , 相干时间内共进行 L 次信道估计。上述参数间具有如下关系:

$$T_k = L \cdot T_l \quad (9)$$

$$R_s = \frac{L \cdot n_k}{T} \quad (10)$$

其中, R_s 为密钥速率, n_k 为每次信道估计后可提取的新的密钥长度。

Shannon^[16]指出, 实现“完美保密”的条件是“一次一密”, 此时需满足密钥 K 的长度不小于明文的长度, 即

$$H(K) \geq H(M) \quad (11)$$

其中, $H(\cdot)$ 表示随机变量的熵。根据上述条件, 相干时间内的可达“一次一密”速率可表示为

$$R_{k,t} = \min \left\{ \frac{R_b T_t}{T}, \frac{R_s T_k}{T} \right\} \quad (12)$$

其中, R_b 代表数据传输速率。

因此, 通过改变相干时间内 T_t 和 T_k 的时间占比, 式(12)中的可达“一次一密”速率存在最优解, 该最优化问题可表示为

$$\begin{aligned} & \max R_{k,t} \\ & \text{约束条件} \begin{cases} 0 \leq T_k \leq T, 0 \leq T_t \leq T \\ L \cdot n_k \geq T_t \cdot R_b \\ T_t + L \cdot T_t \leq T \end{cases} \end{aligned} \quad (13)$$

式(13)所得最优解为当前场景下的“一次一密”最优速率。由于该最优化问题复杂度很低, 因此可用穷举搜索方法进行简单求解。基于 RIS 的密钥生成方法具体实现步骤如下:

- (1) BS 控制 RIS 的反射单元系数随机变化;
- (2) BS 与合法用户 k 互发导频进行第 i 次信道估计, 分别得到信道 $h_{b,k,i}$ 的估计值 $\tilde{h}_{b,k,i}$ 和 $\tilde{h}_{k,b,i}$;
- (3) 根据式(13), 对相干时间内的密钥生成和数据传输进行时间上的联合最优化, 得到当前场景下的“一次一密”最优速率以及此时的信道估计次数 L ;
- (4) 根据步骤(3)求得的 L , 重复步骤(1)和步骤(2);
- (5) 经过 L 次信道估计, BS 与合法用户 k 分别获得随机源 $\tilde{H}_{b,k}$ 和 $\tilde{H}_{k,b}$, 并通过量化、信息协商、隐私放大等步骤生成对称密钥。

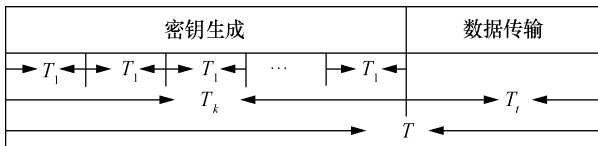


图2 密钥生成与数据传输时隙分布
Figure 2 Key generation and data transmission time slot distribution diagram

4 理论分析

4.1 安全性分析

在上述的密钥生成过程中, 假设 Eve 采用与

合法用户相同的模式进行密钥生成。首先, Eve 和 BS 进行多次信道估计后, 获得了自身与 BS 和 RIS 之间信道 $h_{b,e}$ 的估计值 $\tilde{H}_e$; 然后, Eve 采用同样的方法从信道中提取密钥。

由于 Eve 与合法用户 k 的距离在半波长以上, 信道之间没有相关性, 所以有:

$$I(\tilde{H}_{b,k}; \tilde{H}_e) \approx I(\tilde{H}_{k,b}; \tilde{H}_e) \ll I(\tilde{H}_{b,k}; \tilde{H}_{k,b}) \quad (14)$$

当 BS 和合法用户 k 从共享随机源 $(\tilde{H}_{b,k}; \tilde{H}_{k,b})$ 中提取密钥时, 存在部分信息是窃听方能够窃取到的, 因此就导致了密钥的不安全性^[22]。随着 RIS 反射单元的个数 N 逐渐增大, 窃听者窃取到的共享随机源信息 $I(\tilde{H}_{b,k}; \tilde{H}_e)$ 和 $I(\tilde{H}_{k,b}; \tilde{H}_e)$ 不断减小, 密钥的安全性不断增加。

定理 1 假设 RIS 反射单元个数为 N , 当发送总功率保持不变, RIS 反射单元个数趋近于无穷大时, 合法方的密钥源与窃听方的密钥源的互信息量为 0, 窃听方无法观察到任何共享随机源互信息。

证明 为便于表述, 令

$$\begin{cases} \tilde{Y} = \tilde{H}_{k,b} \\ \mathbf{Z} = \tilde{H}_e \\ \tilde{Z} = \tilde{H}_{b,e} \end{cases} \quad (15)$$

其中, $\mathbf{H}_e = [h_{b,e,1}, h_{b,e,2}, \dots, h_{b,e,L}]^T$ 。窃听方根据接收到的信号所得到的信道估计值为

$$\tilde{\mathbf{Z}} = \mathbf{Z} + \mathbf{n}_e \quad (16)$$

$\tilde{Y} \rightarrow \mathbf{Z} \rightarrow \tilde{\mathbf{Z}}$ 构成马尔可夫链, 根据文献[23]与定理 1 可得:

$$\mathbf{R}_{\tilde{Y}\tilde{\mathbf{Z}}} = \lim_{N \rightarrow \infty} \mathbf{E}[\tilde{\mathbf{Y}}\tilde{\mathbf{Z}}^H] = 0 \quad (17)$$

其中, $\mathbf{R}_{\tilde{Y}\tilde{\mathbf{Z}}}$ 为协方差矩阵, 即 $\tilde{Y}$ 和 $\mathbf{Z}$ 的协方差矩阵为零矩阵。 $\tilde{Y}$ 和 $\mathbf{Z}$ 之间的互信息可以由式(18)表示。

$$I(\tilde{Y}; \mathbf{Z}) = \text{lb} \left| \frac{\mathbf{R}_Z}{\mathbf{R}_Z - \mathbf{R}_{\tilde{Y}\tilde{\mathbf{Z}}} \mathbf{R}_Y^{-1} \mathbf{R}_{\tilde{\mathbf{Z}}\tilde{Y}}} \right| = 0 \quad (18)$$

由马尔可夫链性质 $I(\tilde{Y}; \tilde{\mathbf{Z}}) \leq I(\tilde{Y}; \mathbf{Z})$ 可得:

$$I(\tilde{Y}; \tilde{Z}) = 0 \quad (19)$$

因此, 在定理 1 的情况下, 窃听者无法获取任何共享随机源互信息。证毕。

所以,

$$\lim_{N \rightarrow \infty} I(\tilde{H}_{b,k}; \tilde{H}_e) = \lim_{N \rightarrow \infty} I(\tilde{H}_{k,b}; \tilde{H}_e) = 0 \quad (20)$$

4.2 密钥速率和密钥容量

假设 BS 和合法用户 k 生成密钥 $\mathbf{k}$ 的可达密钥速率为 R_s , 则对于 $\forall \varepsilon > 0$ 和充分大的 n , R_s 和 $\mathbf{k}$ 需要满足以下关系:

$$\begin{cases} \Pr I\{\mathbf{k} \neq \mathbf{k}'\} \leq \varepsilon \\ \frac{1}{n} I(\mathbf{k}; \gamma) \leq \varepsilon \\ \frac{1}{n} H(\mathbf{k}) \geq R_s - \varepsilon \\ \frac{1}{n} \log |\kappa| \leq \frac{1}{n} H(\mathbf{k}) + \varepsilon \end{cases} \quad (21)$$

其中, κ 表示密钥空间, $\mathbf{k}, \mathbf{k}' \in \kappa$, $|\kappa|$ 是 κ 的基数即密钥空间的大小, γ 代表密钥协商过程中发送的协商信息, n 为密钥源符号长度。

参考文献[24]可知, 满足式(2)的可达密钥速率为

$$R_s = \lim_{\Delta \rightarrow 0} \frac{I(\tilde{H}_{b,k}; \tilde{H}_{k,b} | \tilde{H}_e)}{T} \quad (22)$$

在此基础上, 密钥容量 C_s 定义为最大密钥速率^[25], 本文所提方法的 C_s 具有以下上下界:

$$\begin{aligned} C_s &\leq \min \left[I(\tilde{X}; \tilde{Y}), I(\tilde{X}; \tilde{Y} | \tilde{Z}) \right] \leq \\ &\min \left[I(\tilde{H}_{b,k}; \tilde{H}_{k,b}), I(\tilde{H}_{b,k}; \tilde{H}_{k,b} | \tilde{H}_e) \right] \quad (23) \\ C_s &\geq \max \left[I(\tilde{Y}; \tilde{X}) - I(\tilde{Z}; \tilde{X}), \right. \\ &I(\tilde{X}; \tilde{Y}) - I(\tilde{Z}; \tilde{Y}) \geq \\ &\max \left[I(\tilde{H}_{k,b}; \tilde{H}_{b,k}) - I(\tilde{H}_e; \tilde{H}_{b,k}), \right. \\ &\left. I(\tilde{H}_{b,k}; \tilde{H}_{k,b}) - I(\tilde{H}_e; \tilde{H}_{k,b}) \right] \quad (24) \end{aligned}$$

5 仿真结果

为了验证所提方法的可行性和有效性, 本文在 MATLAB R2016a 环境下进行了一系列的仿真

实验。其中, 式(22)中的互信息采用与文献[26]相同的 ITE 工具箱 (information theoretical estimator toolbox) 计算得出, 并假设收发端均进行数字信号处理, 采用 16 bit 量化。本文使用蒙特卡洛方法进行 10 000 次实验, 每次实验都随机产生信道和噪声数据, 确保了实验的准确性。

5.1 密钥速率

本小节在相同环境下, 对本文所提的基于 RIS 的密钥生成方法以及现有的中继辅助方法^[4]、随机信号流方法^[23]和随机数方法^[27]的可达密钥速率进行了对比, 并且仿真分析了不同条件下的可达密钥速率及其影响因素。

5.1.1 密钥速率对比

将本文所提方案与已有方案的可达密钥速率进行对比, 仿真结果如图 3 所示。在仿真实验中, 可达密钥速率利用互信息 $I(\tilde{X}; \tilde{Y} | \tilde{Z})$ 计算, Eve 采用与合法通信双方相同的方法进行密钥生成。其中, 中继辅助方法利用中继发送辅助信息^[4], 通过增加共享随机源中互易信道个数提高密钥速率; 随机信号流方法利用发送方在多天线上发送相互独立的随机信号流, 将接收天线上的叠加随机信号作为共享随机源提取密钥^[23], 通过信号流的随机性提高密钥速率。随机数方法由合法通信双方分别生成随机数然后共享^[27], 利用随机数的随机性提高密钥速率。

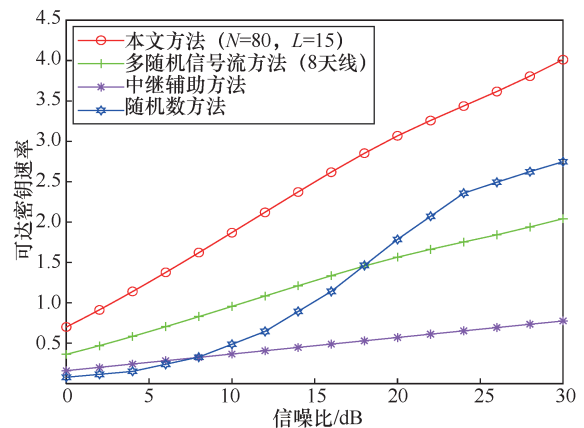


图 3 密钥速率对比
Figure 3 Secret key rates comparison

如图 3 所示, 本文所提方法与其他方法相比, 在密钥速率上有着明显的优势。与中继辅助方法

相比, 本文方法利用 RIS 提高了信道的个数和随机性, 并且增加了相干时间内信道估计的次数; 与随机信号流方法相比, 本文方法所引入的 RIS 具有大量反射单元且每个反射单元都对应一个独立的反射链路, 增加了信号流的数量; 与随机数方法相比, 准静态信道会导致窃听者易于通过随机信号窃取部分共享随机源的信息, 而本文方法的共享随机源由大量快变信道组成, 在合法信道独立于窃听信道的情况下, 几乎不存在密钥源信息的泄露。因此, 本文方法具有较高的可达密钥速率。

5.1.2 密钥速率影响因素

影响密钥速率的因素有信噪比 SNR、RIS 反射单元个数 N 以及相干时间内的信道估计次数 L 。图4、图5和图6分别展示了密钥速率与 SNR、 N 和 L 之间的关系。

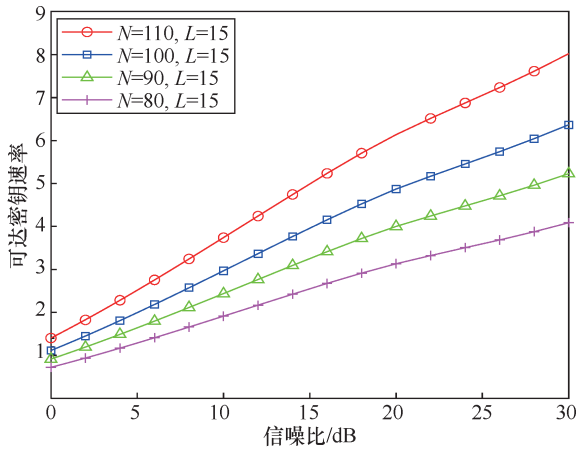


图4 密钥速率随信噪比变化曲线

Figure 4 The graph of secret key rate against signal-to-noise ratio

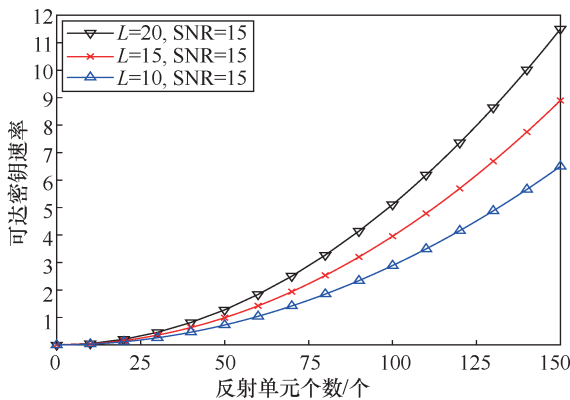


图5 密钥速率随 RIS 反射单元个数变化曲线

Figure 5 The graph of secret key rate against the number of RIS reflection units

如图4、图5和图6所示, 本文方法的密钥速率随着 SNR、 N 和 L 的增加而增加。当信噪比为 15 dB、反射单元个数为 80、90、100、110 时, 每次信道估计可产生的密钥长度分别为 0.058 3 bit、0.108 4 bit、0.134 4 bit、0.167 6 bit。

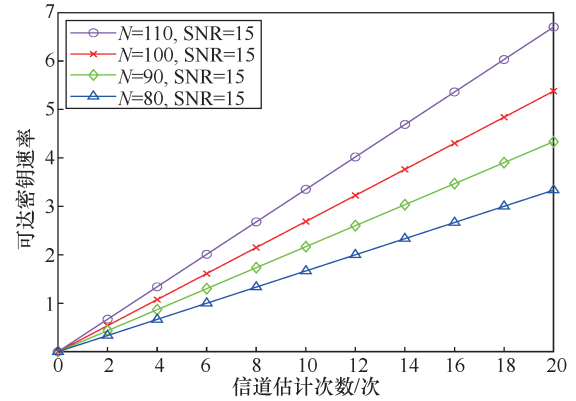


图6 密钥速率随信道估计次数变化曲线

Figure 6 The graph of secret key rate against the number of channel estimations

5.2 密钥安全性分析

本小节对 4.1 节中的定理 1 进行了仿真证明, 仿真结果如图 7 所示。仿真表明, RIS 反射单元的个数 N 越大, 合法通信双方的共享随机源互信息越大, 窃听者窃取共享随机源互信息的难度越大, $I(\tilde{Y}; \tilde{Z})$ 越小, 密钥越安全。

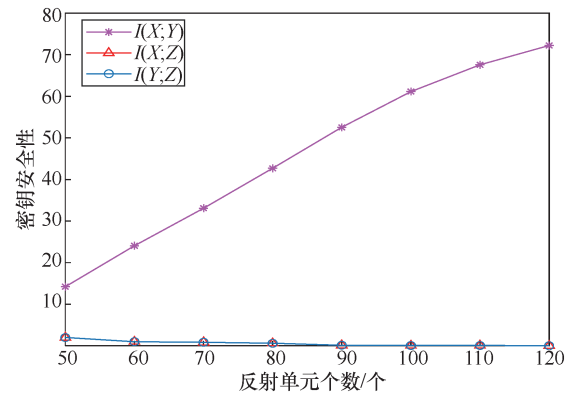


图7 密钥安全性随 RIS 反射单元个数变化曲线

Figure 7 The graph of key secret against the number of RIS reflection units

5.3 “一次一密”速率

本小节对 3.4 节所提的“一次一密”最优化设计进行了仿真分析。首先, 定义时间利用率 $\tau = T_k / T$, 表示密钥生成时间 T_k 占总相干时间 T 的比例。定义 τ_m 表示使用最优化方案后得到的最优时间利用率, 定义 $\tau_{0.5}$ 表示 $\tau = 0.5$ 的一般情况。

基于以上定义, 本文分别在相干时间为 150 ms、120 ms 和 90 ms 的条件下, 以 10 为间隔对时间进行一维单向搜索, 对不同信噪比下的可达“一次一密”速率进行了仿真实验, 结果如图 8 所示。由图可知, 随着信噪比的增加, “一次一密”速率因密钥速率的增加而增加。并且, 通过最优化方案得到的“一次一密”最优速率明显高于一般情况下的可达“一次一密”速率, 这表示本文所提的最优化方案可实现最大传输速率的“一次一密”。

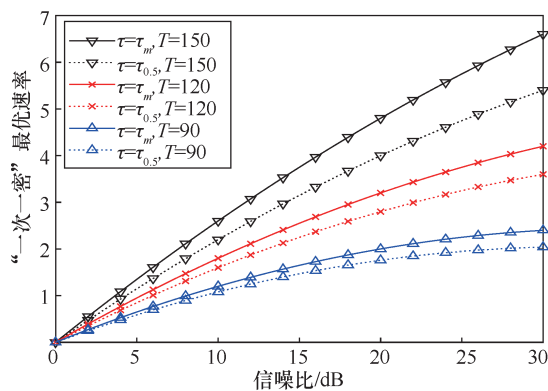


图 8 “一次一密”速率随信噪比变化曲线
Figure 8 The graph of one-time pad rate against varies with signal-to-noise ratio

6 结束语

本文主要研究了物联网通信场景中准静态场景下的密钥生成方法, 针对准静态场景中信道随机性差导致密钥速率低的问题, 提出了基于 RIS 的密钥生成方法。在该方法中, 利用 BS 控制 RIS 反射系数的不断变化, 构造快速变化的信道, 并将复合 CSI 作为共享随机源提取密钥。同时, 本文在此基础上进行了密钥生成与数据传输的联合最优时间分配设计, 在密钥生成时间与数据传输时间相匹配时, 实现了最大传输速率的“一次一密”。实验仿真表明, 本文所提方法的密钥速率高于现有的中继辅助方法、随机信号流方法和随机数方法, 并且随着 RIS 反射单元个数和相干时间内信道估计次数的增加, 密钥速率会有进一步的提高。本文所提的基于 RIS 的密钥生成方法, 为准静态场景下的密钥生成问题提供了一个良好的解决方案, 并且为超材料技术在物理层安全中的应用提供了一条新的思路。

参考文献:

- [1] 李古月, 俞佳宝, 胡爱群. 基于设备与信道特征的物理层安全方法[J]. 密码学报, 2020, 7(2): 224-248.
LI G Y, YU J B, HU A Q. Physical layer security method based on device and channel characteristics[J]. Journal of Cryptography, 2020, 7(2): 224-248.
- [2] MADISEH M, NEVILLE S, MC GUIRE M. Applying beamforming to address temporal correlation in wireless channel characterization based secret key generation[J]. IEEE Transactions on Information Forensics Security, 2012, 7(4): 1278-1287.
- [3] MOARA-NKWE K, SHI Q, LEE G M, et al. A novel physical layer secure key generation and refreshment scheme for wireless sensor networks[J]. IEEE Access, 2019, 6: 11374-11387.
- [4] 肖帅芳, 郭云飞, 白慧卿, 等. 面向物联网准静态信道的中继协作密钥生成方法[J]. 电子与信息学报, 2013(6): 1344-1350.
XIAO S F, GUO Y F, BAI H Q, et al. A method for generating a relay cooperative key for quasi-static channels of the internet of things[J]. Journal of Electronics and Information, 2013, (6): 1344-1350.
- [5] YANG B, WANG W, AND YIN Q. Secret key generation from multiple cooperative helpers by rate unlimited public communication[C]//IEEE International Conference on Acoustics, Speech and Signal Processing. 2014: 8183-8187.
- [6] LOU Y, JIN L, ZHONG Z, et al. Secret key generation scheme based on MIMO received signals spaces[J]. Scientia Sinica Information, 2016, 47(3): 362-373.
- [7] JIN L, ZHANG S, LOU Y, et al. Secret key generation with cross multiplication of two-way random signals[J]. IEEE Access, 2019(99):1.
- [8] TAKAYUKI S, HISATO I, AND HIDEICHI S. Physical-layer secret key agreement in two-way wireless relaying systems [J]. IEEE transactions on Information Forensics and Security, 2011, 6(3): 650-660.
- [9] 魏浩, 郑宝玉, 候晓赞, 等. 基于放大转发的双向中继信道密钥生成[J]. 电子与信息学报, 2013, (6): 1344-1350.
WEI H, ZHENG B Y, HOU X Y, et al. Two-way relay channel key generation based on amplification and forwarding[J]. Journal of Electronics and Information, 2013, (6): 1344-1350.
- [10] WU Q, ZHANG R. Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network[J]. IEEE Communications Magazine, 2020, 58(1): 106-112.
- [11] ZHANG L, CASTALDI G, GALDI V, et al. Space-time-coding digital metasurfaces[C]//2019 Thirteenth International Congress on Artificial Materials for Novel Wave Phenomena (Metamaterials). 2019: 4334.
- [12] ZHOU G, PAN C, REN H, et al. Robust beamforming design for intelligent reflecting surface aided MISO communication systems[J]. IEEE Wireless Communication Letters, 2020, (99): 1.
- [13] GUO H, LIANG Y C, CHEN J, et al. Weighted sum-rate maximization for intelligent reflecting surface enhanced wireless networks[C]//2019 IEEE Global Communications Conference. 2019.
- [14] BJRNSEN E, SANGUINETTI L. Demystifying the power scaling law of intelligent reflecting surfaces and metasurfaces[J]. 2019

- IEEE 8th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), 2019: 549-553.
- [15] DONG L, WANG H M. Enhancing secure mimo transmission via intelligent reflecting surface[J]. IEEE Transactions on Wireless Communications, 2020.
- [16] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.
- [17] CHEN J, LIANG Y C, PEI Y, et al. Intelligent reflecting surface: a programable wireless environment for physical layer security[J]. IEEE Access, 2019, 7: 82599-82612.
- [18] YU X, XU D, SCHOBBER R. Enabling secure wireless communications via intelligent reflecting surfaces[C]//2019 IEEE Global Communications Conference (GLOBECOM).
- [19] WU Q, ZHANG S, ZHENG B, et al. Intelligent reflecting surface aided wireless communications: a tutorial[J]. arXiv: 2007.02759, 2020.
- [20] ZHAN F R, YAO N M, GAO Z G, et al. Efficient key generation leveraging wireless channel reciprocity for MANETs[J]. Journal of Network and Computer Applications, 2018, (103): 18-28.
- [21] BENNETT C H, BRASSARD G, CREPEAU C, et al. Generalized privacy amplification[J]. IEEE Transactions on Information Theory, 1995, 41(6): 1915-1923.
- [22] PASOLINI G, DARDARI D. Secret key generation in correlated multi-dimensional Gaussian channels[C]//2014 IEEE International Conference on Communications. 2014: 2171-2177.
- [23] 金梁, 蔡奥林, 黄开枝, 等. 基于多随机信号流的密钥生成方案[J]. 电子与信息学报, 2019, 41(6): 1405-1412.
- JIN L, CAI A L, HUANG K Z, et al. Key generation scheme based on multiple random signal streams[J]. Journal of Electronics and Information, 2019, 41(6): 1405-1412.
- [24] CSISZAR I, NARAYAN P. Common randomness and secret key generation with a helper[J]. IEEE Transactions on Information Theory, 2000, 46(2): 344-366.
- [25] 楼洋明, 金梁, 钟州, 等. 基于 MIMO 接收信号空间的密钥生成方案[J]. 中国科学 F 辑, 2017, 47(3): 362-373.
- LOU Y M, JIN L, ZHONG Z, et al. Key generation scheme based on MIMO receiving signal space [J]. Science in China Series F, 2017, 47(3): 362-373.
- [26] XIAO S, GUO Y, HUANG K, et al. Cooperative group secret key generation based on secure network coding[J]. IEEE Commun Lett, 2018, 22(7): 1466-1469.
- [27] ALDAGHRI N, MAHDAVIFAR H. Physical layer secret key generation in static environments[J]. IEEE Trans Inform Forensic Secur, 2020, 15: 2692-2705.

[作者简介]



郝一诺 (1997-), 女, 江苏徐州人, 信息工程大学硕士生, 主要研究方向为无线物理层安全。



金梁 (1969-), 男, 北京人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为移动通信技术、阵列信号处理、无线物理层安全。



黄开枝 (1973-), 女, 安徽滁州人, 博士, 信息工程大学教授、博士生导师, 主要研究方向为宽带移动通信与异构网络安全、无线物理层安全。



肖帅芳 (1989-), 男, 河南许昌人, 博士, 信息工程大学助理研究员, 主要研究方向为无线物理层安全。