DOI:10.13878/j.cnki.jnuist.20230714001

王丹[1]　方磊[1]　何斌[1]　陈发堂[1]

准静态环境下的回溯加扰密钥生成算法

摘要

物理层安全技术利用无线信道环境动态生成密钥,但在准静态环境中,信道变换缓慢导致密钥的随机性及安全性不足,因而提出一种回溯加扰密钥生成算法(Backtracking Scrambled Key Generation,BSKG).首先,拆分信道系数的实部虚部量化以生成更长的密钥.调和后,再利用本次密钥与上一次密钥间的不一致索引总和生成扰码并与本次密钥加扰.仿真结果表明,较现有的多维信息、添加人工随机性的密钥生成方法,本文算法具有更高的密钥生成速率和安全性,且随"一次一密"密钥生成次数的增加,即使被窃听到较相关的信道系数,密钥泄露率仍接近0.5.利用语义安全和信息论不等式分别估计一般及恶劣信道条件成功窃听的概率上界及其随密钥生成次数N的变化情况,给定某些参数,得到这两种情况下的概率上界分别为2^{-77N}和2^{-23N}.

关键词

物理层安全;一次一密;准静态环境;回溯加扰

中图分类号 TN918.82

文献标志码 A

收稿日期 2023-07-14

资助项目 重庆市自然科学基金(cstc2021jcyj-msxmX0454)

作者简介

王丹,女,博士,正高级工程师,研究方向为移动通信、物联网、信号处理等.wangdan@cqupt.edu.cn

方磊(通信作者),男,硕士生,主要研究方向为物理层安全技术.1513109153@qq.com

1 重庆邮电大学 通信与信息工程学院,重庆,400065

0 引言

物理层加密技术利用无线链路特性生成密钥.其中,无线信道因其时变性[1]、互易性[2]可作为双方密钥的随机性来源,保证在短时间内生成一致密钥而无需额外的计算开销,或分发管理的基础设施.此外,在多径散射环境中,如果窃听者与合法用户之间的距离大于半个波长,则可近似认为两者接收同一信号所经历的信道完全不相关[3],从而保证其安全性.

然而,在准静态环境,如空旷地区或一些室内场景,信道变化缓慢、相干时间较长,使得连续生成密钥之间以及单次生成密钥内部存在一定的相关性,导致密钥生成不满足"一次一密"保密条件[4-5],密钥生成速率降低,窃听端也更易获取与合法端相关的信道信息,系统的安全性也有所下降.

针对准静态环境存在的问题,目前的研究已经取得了一些进展.密钥的生成速率大多借助时域、频域、相位等多维信道信息来提高.例如:文献[6]不仅使用信道系数的幅度、相位生成密钥,还从对应最高增益的子信道的索引生成随机密钥比特以提高生成速率;文献[7]使用时频空维度的多入多出(Multiple-In Multiple-Out,MIMO)信道以生成长度更长的密钥.此外,通过增加中继或智能反射面(Reconfigurable Intelligent Surface,RIS)辅助生成密钥也是提高密钥生成速率的重要方法.文献[8]研究了双向中继生成密钥,提出4种基于放大转发的密钥生成方案,通过中继增加信道探测数量进而提高密钥生成速率;文献[9]使用缓冲器和中继存储每次生成密钥中未使用的比特位,以避免出现某次信道探测生成的密钥位长度不足的问题;文献[10]借助多个中继生成密钥,并研究了中继不可信时的密钥生成方案,可在较大范围内实现较高的密钥生成速率;文献[11-12]通过在两端添加RIS,利用RIS的捷变特性构造快速变化的信道,从而使密钥生成不受制于自然信道变化速度.然而,通过多维信息或增加准静态环境下的信道仍无法有效避免静态问题,且MIMO信道的增加将导致计算复杂度和时间消耗的增加.而添加中继或是RIS又要考虑部署及能耗问题,如果RIS或中继被窃听者操控,系统的安全性将得不到保证.针对密钥的随机性,引入人工随机源提高密钥随机性是目前的有效手段.文献[13-14]提出在直接型和中继型2种密钥生成场景下,在信道探测阶段发射人工随机源扰动信道,双方以4次交互后的信道系数生

成密钥;文献[15]提出一种高效的人工随机性及预编码辅助密钥生成方法,并验证了迫零及最大传输比率2种预编码技术下的有效性;文献[16]设计预编码矩阵,通过广播随机控制设备的接收天线并量化密钥,提高密钥的随机性;文献[17]则将信道探测系数的相位量化为扰码初始值,生成扰码序列对密钥进行加扰;文献[18]基于随机滤波和随机天线调度改善信道参数的动态特性,同时使用自适应量化和霍特林变换提取更多的随机比特生成密钥.但这些添加人工随机源的方法,都将造成双方互易性的降低,使得双方密钥不一致率增加,这势必会给信息调和带来压力并增加双方交互,准静态环境下交互的增加将导致可能的风险显著增加,系统的安全性降低.同时,采用多天线及预编码技术的密钥性能需在MIMO场景下才能充分展现,这又使得设备的硬件开销显著增加.

基于前人的研究分析,本文提出一种回溯加扰密钥生成算法(Backtracking Scrambled Key Generation,BSKG),做出的主要工作如下:

1)密钥调和后,双方利用上次通信的密钥与当前密钥,计算不一致索引总和,生成扰码序列,将其与当前密钥异或.一方面,加扰有效地提高了随机性,另一方面,双方仅需保存上一次密钥获得一致扰码初始值而无需交互,且扰码初始值不断变化,窃听端要窃取密钥,不仅需要窃取本次探测的信道系数,还需要窃取扰码初始值,而要窃取初始值又需以完全窃取上次通信密钥为保证,窃取上一次密钥则与此同理,因而有效地提高了系统安全性.

2)考虑窃听端可获得与合法端较为相关信道信息的情况,通过语义安全和信息论不等式推导了所提算法窃听端成功窃听的概率上限.给定某些参数,结果表明,即使窃听端能够获得与合法端极为相关的信道信息,随着密钥生成次数的增加,窃听成功的概率也将快速下降.

3)通过仿真验证,算法的密钥泄露率和重复率始终接近理想情况,且因拆分信道系数的实部虚部生成密钥,相较现有算法,本文算法还具有较高的密钥生成速率和较低的密钥不一致率,并通过了NIST(National Institute of Standards and Technology)随机性测试.

1 系统模型及算法

1.1 系统模型

针对准静态环境,建立模型如图1所示.合法通信双方为Alice、Bob,存在一个窃听者Eve,且物理位置更靠近Bob.信道模型为准静态瑞利衰落信道,通信系统模型为时分双工模式下的SISO(Single-Input Single-Output,单入单出)-OFDM(Orthogonal Frequency-Division Multiplexing,正交频分复用)系统.假设合法双方需发N次信息,根据"一次一密"条件则需至少生成N次密钥.

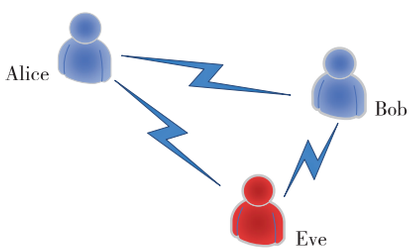

图1 系统模型

Fig. 1 System model

1.2 密钥生成算法

算法使用信道系数的实部虚部量化密钥,并在双方信息调和后,进行回溯加扰,提高密钥的随机性和安全性.密钥生成具体步骤如下:

1.2.1 信道探测与估计

为获得信道状态信息,在相干时间内,Alice和Bob分别发送导频信号$x_a(t_1)$和$x_b(t_2)$,双方接收到的信号分别为

$$y_B = h_{AB}(t_1) * x_a(t_1) + n_{AB_1}(t_1), \tag{1}$$

$$y_A = h_{BA}(t_2) * x_b(t_2) + n_{BA_1}(t_2). \tag{2}$$

分别做信道估计得到信道系数:

$$\tilde{h}_{AB} = h_{AB}(t_1) + n_{AB_2}(t_1), \tag{3}$$

$$\tilde{h}_{BA} = h_{BA}(t_2) + n_{BA_2}(t_2). \tag{4}$$

其中,$*$表示卷积,信道系数是均值为0方差为σ_n^2的高斯分布,噪声为独立同分布的加性高斯白噪声.

1.2.2 特征量化

量化即将信道特征转换为密钥比特,算法将每个子载波的实部和虚部分别量化,以提高密钥的生成速率,量化步骤如下:

1)假设双方获得的频域信道系数为$H \in \mathbf{C}^{1\times M}$,即$H=[h_1,h_2,\cdots,h_i,\cdots,h_M]$,其中,$M$为子载波数,$R(h_i)$和$I(h_i)$分别表示第$i$个子载波系数的实部和虚部,则有$R(H)=[R(h_1),R(h_2),\cdots,R(h_i),\cdots,R(h_M)]$,$I(H)=[I(h_1),I(h_2),\cdots,I(h_i),\cdots,I(h_M)]$.

2)计算子载波系数的范围并设置$\xi=2^{\varphi}$个均匀量化区间,量化得到初始密钥$K_Q \in \mathbf{C}^{1\times 2M}$.

例如:$\varphi = 1$,使用信道系数幅度的均值 mean$R$、mean$I$ 为门限,量化密钥:

$$K_{\mathrm{R},i} = \begin{cases} 0, & R(h_i) \geqslant \mathrm{mean}R; \\ 1, & R(h_i) < \mathrm{mean}R. \end{cases} \tag{5}$$

$$K_{\mathrm{I},i} = \begin{cases} 0, & I(h_i) \geqslant \mathrm{mean}I; \\ 1, & I(h_i) < \mathrm{mean}I. \end{cases} \tag{6}$$

$$K_{\mathrm{Q}} = [K_{\mathrm{R},1}, K_{\mathrm{I},1}, K_{\mathrm{R},2}, K_{\mathrm{I},2}, \cdots, K_{\mathrm{R},M}, K_{\mathrm{I},M}]. \tag{7}$$

1.2.3 信息调和

本文采用文献[19]所述的基于纠错编码的信息调和方案,简而言之,即为 Alice 将量化后的密钥分组并基于纠错编码生成协商信息,Bob 收到后利用纠错编码的纠错能力进行纠错,最终实现双方密钥一致.

1.2.4 回溯加扰算法

设调和后的一致密钥为 $K_1 = [K_{1,1}, K_{1,2}, \cdots, K_{1,M_1}]$,$N$ 为双方密钥生成次数,双方回溯用于第 $N-1$ 次通信加密的一致密钥为 $K_{L_1} = [K_{L_1,1}, K_{L_1,2} \cdots, K_{L_1,M_2}]$,生成扰码加扰以提高密钥随机性及安全性,算法具体步骤如下:

1) $N = 1$

双方首次发起密钥生成请求,此时无法回溯,安全性仅依赖于信道的不相关性,因而不用来对信息进行加密.双方进行隐私放大并确认首次密钥一致后更新 K_{L_1},然后重新开始密钥生成.

2) $N > 1$

① 因信息调和及隐私放大将舍弃部分比特导致连续生成密钥的长度不同,即 $M_1 \neq M_2$,取 $M_3 = \min(M_1, M_2)$ 得:

$$K_2 = [K_{1,1}, K_{1,2} \cdots, K_{1,M3}], \tag{8}$$

$$K_{L_2} = [K_{L_1,1}, K_{L_1,2}, \cdots, K_{L_1,M_3}]. \tag{9}$$

② 获取不一致索引总和 α:

$$K_3 = K_2 \oplus K_{L_2}, \tag{10}$$

$$\alpha = \sum_{i=1}^{M_3} iK_{3,i}. \tag{11}$$

③ 将 α 转成二进制比特:

$$\alpha = [C_{1,1}, \cdots, C_{1,j}, \cdots, C_{1,s}], \tag{12}$$

得到 31 位扰码初始值 C_2:

$$C_2 = \begin{cases} [C_{1,1}, \cdots, C_{1,j}, \cdots, C_{1,31}] \in \mathbf{C}^{1\times 31}, s \geqslant 31, \\ [C_{1,1}, \cdots, C_{1,j}, \cdots, C_{1,s}, 0, \cdots, 0] \in \mathbf{C}^{1\times 31}, s < 31. \end{cases} \tag{13}$$

引入 Gold 序列[20],序列由 2 个 m 序列生成,具有良好的随机性.第 1 个 m 序列 p 初始化为 $p(1) = 1$,$p(n) = 0, n = 2, 3, \cdots, 31$;第 2 个 m 序列 q 初始化为 $q(n) = C_2(n)$,$n = 1, 2, \cdots, 31$.当 m 序列长度大于 31 时有:

$$\begin{aligned} p(n+31) &= (p(n+3) + p(n)) \bmod 2, \\ q(n+31) &= (q(n+3) + q(n+2) + \\ &\quad q(n+1) + q(n)) \bmod 2. \end{aligned} \tag{14}$$

生成长度为 M_1 的 Gold 序列 C_3:

$$C_3(n) = (p(n + N_c) + q(n + N_c)) \bmod 2. \tag{15}$$

其中,$N_c = 1\,600$,$n \in [1, M_1]$.

④ 将调和后的密钥 $K_1 \in \mathbf{C}^{1\times M_1}$ 与 C_3 异或得到回溯加扰算法的输出密钥 $K_4 \in \mathbf{C}^{1\times M_1}$.

$$K_4 = K_1 \oplus C_3. \tag{16}$$

1.2.5 隐私放大及一致性检验

为进一步提高密钥安全性及确认最终密钥是否一致,协议使用文献[14]描述的隐私放大及一致性检验方法.此外,双方每次可根据 α 从全域哈希函数集中选择一致哈希函数而无须预先沟通或是交互.

双方在确认密钥一致后将 K_{L_1} 更新为本次密钥,以便下次回溯加扰.若不一致则密钥生成失败,丢弃本次密钥重新生成.

2 安全分析

这部分将给出一般以及恶劣两种信道条件下(两者的区别在于窃听端与合法端信道系数的相关程度),窃听者成功窃取到第 N 次合法密钥的概率上限及其变化规律.

信道探测阶段,Eve 已经通过监听公共信道获得了部分有关密钥生成的信息:

$$y_{\mathrm{E}} = h_{\mathrm{AE}}(t_1) * x_{\mathrm{a}}(t_1) + n_{\mathrm{AE}_1}(t_1), \tag{17}$$

$$\tilde{h}_{\mathrm{AE}} = h_{\mathrm{AE}}(t_1) + n_{\mathrm{AE}_2}(t_1). \tag{18}$$

一般来说,窃听者与合法信道相距大于半波长 $\lambda/2$ 时,他们将经历完全不相关的衰落信道.然而,在准静态环境信道变化缓慢,Eve 通过监听信道获得的信道系数与合法端仍可能有一定的相关性,系统的安全性也将有所下降.

Eve 与合法端所得共享随机性的互信息量是一种信息论的安全性度量方法.假设量化的影响可以忽略不计,考虑到 Eve 更加靠近 Bob,则只需考虑 $\tilde{h}_{\mathrm{AE}}$ 与 $\tilde{h}_{\mathrm{AB}}$,那么合法方与 Eve 的互信息计算如下:

定义 Bob 端以及 Eve 端任意子载波 k 上的衰落系数分别为 $h_{\mathrm{b},k} = h_{\mathrm{b},k,\mathrm{R}} + \mathrm{j}h_{\mathrm{b},k,\mathrm{I}}$ 和 $h_{\mathrm{e},k} = h_{\mathrm{e},k,\mathrm{R}} + \mathrm{j}h_{\mathrm{e},k,\mathrm{I}}$,其中,$h_{\mathrm{b},k,\mathrm{R}}$ 和 $h_{\mathrm{b},k,\mathrm{I}}$ 独立且满足正态分布 $\mathcal{N}(0, \sigma_{\mathrm{b}}^2/2)$,$h_{\mathrm{e},k,\mathrm{R}}$ 和 $h_{\mathrm{e},k,\mathrm{I}}$ 独立且满足正态分布 $\mathcal{N}(0, \sigma_{\mathrm{e}}^2/2)$,则有互信息

$$I(h_{b,k};h_{e,k}) = I(h_{b,k,R} + jh_{b,k,I};h_{e,k,R} + jh_{e,k,I}) = I(h_{b,k,R},h_{b,k,I};h_{e,k,R},h_{e,k,I}) = H_d(h_{b,k,R},h_{b,k,I}) + H_d(h_{e,k,R},h_{e,k,I}) - H_d(h_{b,k,R},h_{b,k,I},h_{e,k,R},h_{e,k,I}). \quad (19)$$

$H_d(\cdot)$ 表示微分熵,式(19)即为互信息的微分熵展开式.引入合法端与窃听端信道的相关系数:

$$\rho = \frac{\mathrm{cov}(h_{b,k},h_{e,k})}{\sqrt{D(h_{b,k})D(h_{e,k})}} = \frac{\mathrm{E}[h_{b,k}h_{e,k}]}{\sqrt{\mathrm{E}[\|h_{b,k}\|^2]\mathrm{E}[\|h_{e,k}\|^2]}}. \quad (20)$$

其中,cov(·)表示变量的协方差,得到以下协方差矩阵:

$$\boldsymbol{\Sigma}_1 = \begin{bmatrix} \sigma_b^2/2 & 0 \\ 0 & \sigma_b^2/2 \end{bmatrix}, \boldsymbol{\Sigma}_2 = \begin{bmatrix} \sigma_e^2/2 & 0 \\ 0 & \sigma_e^2/2 \end{bmatrix}, \quad (21)$$

$$\boldsymbol{\Sigma}_3 = \begin{bmatrix} \sigma_b^2/2 & 0 & \rho\sigma_b\sigma_e/2 & 0 \\ 0 & \sigma_b^2/2 & 0 & \rho\sigma_b\sigma_e/2 \\ \rho\sigma_b\sigma_e/2 & 0 & \sigma_e^2/2 & 0 \\ 0 & \rho\sigma_b\sigma_e/2 & 0 & \sigma_e^2/2 \end{bmatrix}. \quad (22)$$

对于多元高斯随机变量 $\tilde{X} = (X_1,X_2,\cdots,X_n)$,其协方差矩阵为 $\boldsymbol{\Sigma}$,得到随机变量微分熵为 $H_d(X) = \frac{1}{2}\log(\det(2\pi e\boldsymbol{\Sigma}))$,式(19)可进一步化作:

$$I(h_{bk};h_{ek}) = \frac{1}{2}\log(\det(2\pi e\boldsymbol{\Sigma}_1)) + \frac{1}{2}\log(\det(2\pi e\boldsymbol{\Sigma}_2)) - \frac{1}{2}\log(\det(2\pi e\boldsymbol{\Sigma}_3) = \log(\pi e\sigma_b^2) + \log(\pi e\sigma_e^2) - \log((\pi e\sigma_b\sigma_e)^2(1-\rho^2)) = -\log(1-\rho^2). \quad (23)$$

接下来,利用文献[21]中提供的互信息与语义安全度量之间的联系,计算在一般情况下,相关系数 ρ 较小时,窃听端窃听成功的概率上限.

设 N 为双方密钥生成次数,n 为子载波数,ϕ 为量化分辨率,窃听成功的概率为 P_N.在 Eve 未能监听到有效信息的情况下,成功猜测单个子载波比特的概率为 $2^{-2\varphi}$.根据文献[21]中的结论,在 Eve 窃听的信息与合法端信息相关时,对于单个子载波而言,窃听成功的概率最多增加 $\sqrt{2I(h_b;h_e)}$,其中,h_b 和 h_e 分别为 Bob 端以及 Eve 端子载波的信道系数.窃听端从首次生成密钥开始窃听,$N=1$ 时,Eve 能够恢复出所有子载波的概率为 $(2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n$,需要注意的是 $I(h_b;h_e)$ 对于所有子载波都是相同的,如果 Eve 不能恢复所有的共享随机性,则根据协议隐私放大及一致性检验部分的哈希函数性质,正确猜测出所有密钥的概率为 $2^{-\varphi n}$,那么本次密钥生成 Eve 能成功窃听的概率最多为 $(2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n + 2^{-\varphi n}$.

$N > 1$ 时,Eve 不仅需窃取本次信道系数,还需在此之前成功窃取第 $N-1$ 次的一致密钥来获取本次加密的扰码初始值.设成功窃听第 $N-1$ 次密钥的概率为 P_{N-1},则成功窃听第 N 次密钥的概率最大为 $P_{N-1}\cdot((2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n + 2^{-\varphi n})$.以此类推,得到 Eve 成功窃听第 N 次密钥的概率 P_N 的上界为

$$P_N \leqslant P_{N-1}\cdot((2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n + 2^{-\varphi n}) \leqslant P_{N-2}\cdot((2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n + 2^{-\varphi n})^2 \leqslant \cdots \leqslant ((2^{-2\varphi} + \sqrt{2I(h_b;h_e)})^n + 2^{-\varphi n})^N \leqslant ((2^{-2\varphi} + \sqrt{-2\log(1-\rho^2)})^n + 2^{-\varphi n})^N. \quad (24)$$

基于式(24),通过实际数据进一步说明 Eve 窃听成功的概率上界及其随合法双方密钥生成次数的变化规律.假设使用 64 个子载波生成密钥,量化分辨率 $\varphi=2$,在一般条件下,窃听端所能得到的最大相关系数假设为 0.25,由式(23)得互信量为 0.093 1,则一般条件下 Eve 成功窃听第 N 次密钥的概率上界为 2^{-77N},变化规律如图 2 所示.

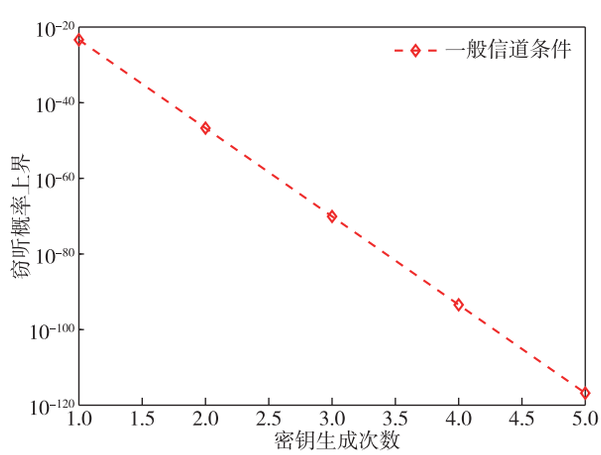

图 2 一般信道条件下的窃听概率上界

Fig. 2 Upper bound on probability of eavesdropping under general channel condition

式(24)已经给出在一般信道条件下,Eve 的窃听概率上界及其随密钥生成次数 N 的变化情况,但对于一些恶劣情况,如某一时刻环境过于静态、Eve

过于靠近合法用户等,其有可能获得与合法端非常相关的信道系数.显然,当相关系数大于 0.54,即互信量大于 0.5 时,对于式(24),将无法得到一个窃听概率的非平凡上界,因此,使用法诺不等式[22]将窃听者成功窃听的概率与子载波量化比特的信息熵联系起来,给出成功窃听的概率上界.

设 N 为密钥生成次数,n 为子载波数,S_k 为第 k 个子载波的量化比特序列,φ 为量化分辨率.将窃听端窃听合法端密钥的过程看作是一个通信过程,合法端可看作编码发送端而窃听端接收(窃听信道系数)经过信道噪声的信息,并进行译码,这样就很容易将译码成功的概率与法诺不等式联系起来,得到一个译码(窃听)成功的概率上界.

$N=1$ 时,基于文献[23]中的不等式及其推论,有:

$$P[S_{e,k}\neq S_k]\geqslant\frac{H(S_k\mid h_{e,k})-1}{\log_2(\mid n\mid)},\tag{25}$$

则窃听者窃听成功的概率 $P[S_{e,k}=S_k]$ 上界为

$$\begin{aligned}P[S_{e,k}=S_k]&\overset{a}{\leqslant}1-P[S_{e,k}\neq S_k]=\\&1-\frac{H(S_k\mid h_{e,k})-1}{\log_2(\mid n\mid)}\overset{b}{=}\\&1-\frac{H(S_k)-I(S_k;h_{e,k})-1}{\log_2(n)}\overset{c}{\leqslant}\\&1-\frac{H(S_k)-I(h_{b,k};h_{e,k})-1}{\log_2(n)}\overset{d}{=}\\&1-\frac{H(S_k)+\log_2(1-\rho^2)-1}{\log_2(n)}.\end{aligned}\tag{26}$$

其中:a 表示法诺不等式;b 表示信息论条件熵展开式;c 中,S_k 是 $h_{b,k}$ 的确定性函数,因此由 $S_k,h_{b,k},h_{e,k}$ 构成马尔可夫链得出;d 可带入式(23)得出.

式(26)对于所有的子载波都是成立且独立的,如果窃听者不能基于监听的信道系数猜测出所有密钥,那么根据协议隐私放大及一致性检验部分的哈希函数性质,其恢复出所有密钥的概率最多为 $2^{-\varphi n}$.因此,本次密钥生成 Eve 能成功窃听的概率最多为

$$\left(1-\frac{H(S_k)+\log(1-\rho^2)-1}{\log(n)}\right)^n+2^{-\varphi n}.$$

$N>1$ 时,Eve 不仅需窃取本次信道系数,还需在此之前成功窃取第 $N-1$ 次的一致密钥来获取本次加密的扰码初始值.设成功窃听第 $N-1$ 次密钥的概率为 P_{N-1},则成功窃听第 N 次密钥的概率最多为

$$P_{N-1}\cdot\left(\left(1-\frac{H(S_k)+\log(1-\rho^2)-1}{\log(n)}\right)^n+2^{-\varphi n}\right).$$

以此类推,成功窃听第 N 次密钥的概率 P_N 的上界为:

$$\begin{aligned}&P_N\leqslant\\&P_{N-1}\cdot\left(\left(1-\frac{H(S_k)+\log(1-\rho^2)-1}{\log(n)}\right)^n+2^{-\varphi n}\right)\leqslant\\&P_{N-2}\cdot\left(\left(1-\frac{H(S_k)+\log(1-\rho^2)-1}{\log(n)}\right)^n+2^{-\varphi n}\right)^2\leqslant\\&\cdots\leqslant\\&\left(\left(1-\frac{H(S_k)+\log(1-\rho^2)-1}{\log(n)}\right)^n+2^{-\varphi n}\right)^N.\end{aligned}\tag{27}$$

基于式(27),通过实际数据进一步说明 Eve 窃听成功的概率上界及其随合法双方密钥生成次数的变化规律.假设使用 64 个子载波生成密钥,量化分辨率 $\varphi=2$,在恶劣条件下,窃听端会得到与合法端非常相关的信道系数,假设 $\rho=0.8$,每个子载波的信息熵可通过 NIST 中的近似熵检测进行估计[24].假设 $H(S_k)\approx3.81$ bit,则恶劣条件下 Eve 成功窃听第 N 次密钥的概率上界为 2^{-23N},变化规律如图 3 所示.

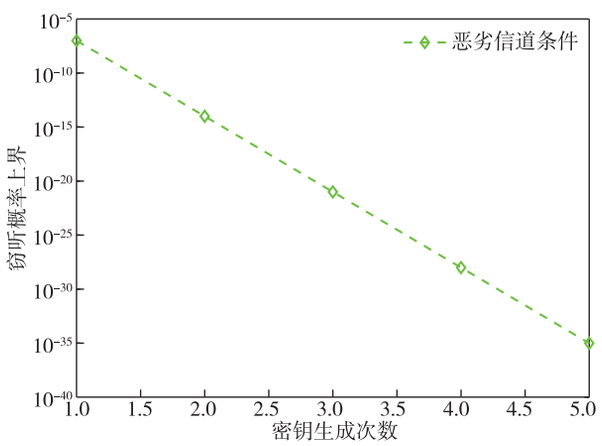

图 3 恶劣信道条件下的窃听概率上界

Fig. 3 Upper bound on probability of eavesdropping under bad channel condition

综上,加扰让 Eve 必须基于监听的信道系数生成与合法端完全一致的密钥,同时,回溯又使得 Eve 还要以窃取之前所有密钥为前提.即使 Eve 获取了与合法端高相关的信道系数,也难以成功窃取密钥,且其概率上界也随着双方密钥生成次数增加而快速降低.

3 仿真分析

将 BSKG 与传统密钥生成(Conventional Key Generation,CKG)[25]、多维信息密钥生成(Joint Key

Generation,JKG)[6]以及加入随机源密钥生成(Induced Randomness Key Generation,IRKG)[14]进行比较,通过仿真结果来分析算法性能.假设任意2个通信节点之间的准静态瑞利衰落信道有9条有效路径,其中考虑了指数衰减功率延迟分布[26].在信号探测阶段,所有算法都使用64个子载波数.

在窃听端,随着环境信噪比的提高,Eve将窃听到与合法信道越来越相关的信道系数,进一步分析算法的安全性能.

3.1 性能指标

密钥生成速率(Key Generation Rate,KGR)描述了每次探测生成的密钥比特与信道特征数量的比值,KGR越高,则密钥生成效率越高,密钥生成越快,通信系统越安全.给出密钥生成速率的公式如下:

$$\mathrm{KGR}=\frac{L}{M}. \tag{28}$$

其中:L表示单次探测生成的有效密钥比特数目(bits);M表示单次探测的信道特征数目(sample).

密钥不一致率(Key Disagreement Ratio,KDR)用于衡量合法通信双方生成密钥的不匹配程度,KDR越低,则调和阶段的交互次数越少,泄露的概率越低,同时密钥生成的成功率越高.给出密钥不一致率公式如下:

$$\mathrm{KDR}=\frac{\sum_{i=1}^{n}\left|K_{\mathrm{A}}(i)-K_{\mathrm{B}}(i)\right|}{M}. \tag{29}$$

其中:K_{A},K_{B}分别为Alice端、Bob端生成的密钥.

密钥泄露率(Key Leakage Rate,KLR)指的是窃听端与合法端密钥一致的比率,是密钥生成算法安全性的重要度量,公式如下:

$$\mathrm{KLR}=1-\frac{\sum_{i=1}^{n}\left|K_{\mathrm{B}}(i)-K_{\mathrm{E}}(i)\right|}{M}. \tag{30}$$

其中:K_{E}为窃听端生成的密钥.根据信息论可知,窃听端密钥与合法端密钥完全不相关时,KLR为0.5.

在准静态环境,信道变化缓慢,连续信道探测生成的密钥可能存在较多相同比特,这对于"一次一密"是不被允许的.密钥重复率(Key Repetition Rate,KRR)可用来衡量连续生成密钥之间的重复比率,公式如下:

$$\mathrm{KRR}=1-\frac{\sum_{i=1}^{n}\left|K_{N}(i)-K_{N-1}(i)\right|}{M}. \tag{31}$$

其中:K_N,K_{N-1}分别为第N次、第$N-1$次生成的密钥.连续生成的密钥重复率越低,则KRR越接近0.5.

密钥随机性通常使用NIST统计测试套件[24]进行测试,该套件测试共有15项,检测序列的相关性、游程、近似熵等特性,以发现可能存在的各种类型的非随机性.对于每个测试而言,如果输出的概率值P大于0.01,则认为该序列是随机的且具有99%的置信度.

3.2 仿真性能

图4、5分别给出了加密算法的KGR、KDR随信噪比的变化曲线.因为BSKG、IRKG拆分信道系数的实部和虚部分别生成密钥,在相同信噪比的情况下,单次信道探测生成的一致比特要高于JKG、CKG算法.IRKG引入随机源,改善随机性的同时也因增加交互引入了更多噪声,导致不一致比特增多,而BSKG在调和后再回溯加扰,保证随机性的同时也不会降低一致率.但随BSKG量化分辨率的提高,KDR较CKG略有增大.

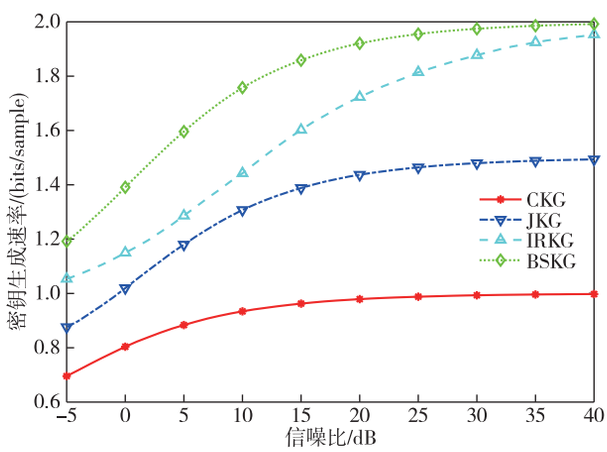

图4 CKG、JKG、IRKG、BSKG的KGR随信噪比的变化情况

Fig. 4 Variations of KGR with signal-to-noise ratio for CKG,JKG,IRKG,and BSKG

图6为加密算法的KLR随信噪比的变化曲线.由于CKG与JKG算法都仅依赖信道的保密性,随着信噪比及Eve窃听的信道系数与合法端相关性的提高,最终导致较高的密钥泄露率.而IRKG虽引入随机源但仍需交互以保证双方获得一致随机信号,在Eve获得逐渐相关信道信息时,泄露率也逐渐增加.对于BSKG而言,通过回溯加扰,一方面,放大了合法端与Eve信道系数差异对密钥生成的影响,即使是1 bit的不同也能使合法端与Eve的密钥完全不同,另一方面,因双方通信次数的增加而不断生成密钥,窃听者

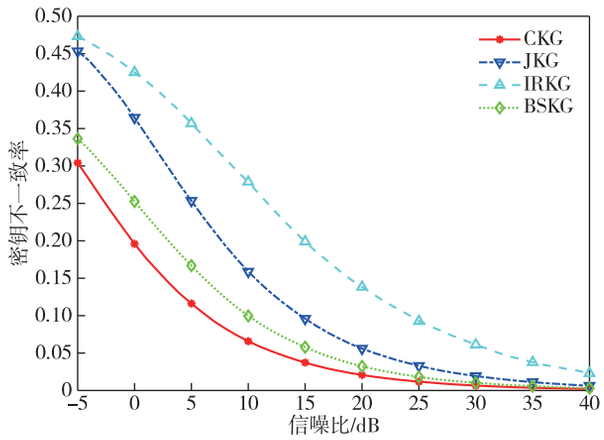

图 5　CKG、JKG、IRKG、BSKG 的 KDR 随信噪比的变化情况

Fig. 5　Variations of KDR with signal-to-noise ratio for CKG, JKG, IRKG, and BSKG

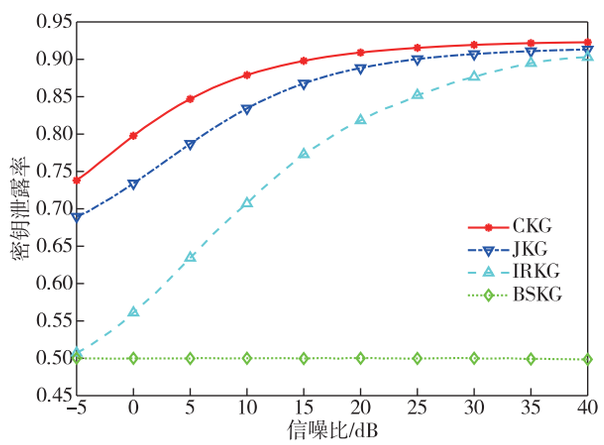

图 6　CKG、JKG、IRKG、BSKG 的 KLR 随信噪比的变化情况

Fig. 6　Variations of KLR with signal-to-noise ratio for CKG, JKG, IRKG, and BSKG

的窃听难度也随之不断加大.随着信噪比以及 Eve 窃听信道系数的相关性不断提高,算法的泄露率始终保持在理想值 0.5,展现了较好的算法安全性能.

图 7 为 KRR 随信噪比的变化曲线.随着信噪比的提高,信道变化逐渐减小,CKG、JKG 算法连续生成密钥之间的重复比特逐渐增多,密钥安全性降低,IRKG 引入随机源提高了密钥随机性,而 BSKG 使用不断变化的扰码加扰,使连续生成密钥之间重复比特率接近 0.5,性能更加稳定.

表 1 为 BSKG 算法使用 NIST 统计测试套件检验随机性的结果.设置静态信道系数运行算法,信噪比为 25 dB,将生成的密钥进行测试.从表 1 中结果可见,序列通过了所有测试,因此,BSKG 算法生成的密钥被认为是随机的且具有 99%的置信度.

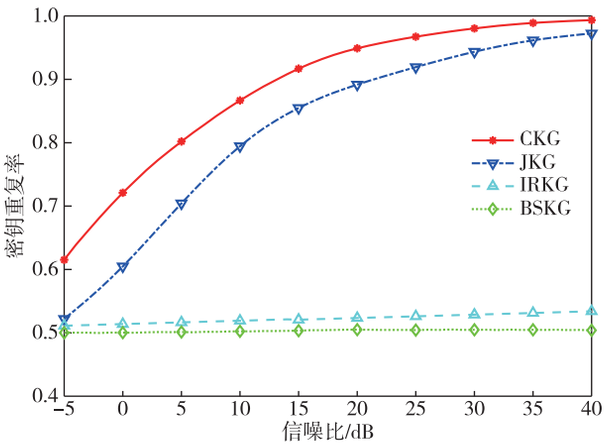

图 7　CKG、JKG、IRKG、BSKG 的 KRR 随信噪比的变化情况

Fig. 7　Variations of KRR with signal-to-noise ratio for CKG, JKG, IRKG, and BSKG

表 1　NIST 测试结果

Table 1　NIST test results

测试项目	*P*-values
Frequency	0.911 4
Block Frequency	0.739 9
Cumulative Sums	0.834 3
Runs	0.213 3
Longest Run	0.148 7
Rank	0.213 3
FFT	0.213 3
Non-Overlapping Template	0.991 4
Overlapping Template	0.739 9
Approximate Entropy	0.275 7
Universal	0.275 7
Random Excursions	0.534 1
Random Excursions Variant	0.350 4
Serial	0.834 3
Linear Complexity	0.739 9

4　结论

回溯加扰算法在不增加双方交互次数以及降低密钥其他性能的基础上,利用上一次密钥与本次密钥的不一致索引总和生成扰码并加扰.一方面,扩大了信道变化对密钥产生的影响,即使信道变化非常缓慢,也不影响密钥生成,使其满足“一次一密”保密条件;另一方面,即使 Eve 能够获得与合法端较为相关的信道系数,回溯加扰也能极大地保证密钥的安全性.仿真结果表明,在准静态环境下,算法具有良好的随机性与安全性.

参考文献
References

[1] Zeng K. Physical layer key generation in wireless networks:challenges and opportunities[J].IEEE Communications Magazine,2015,53(6):33-39
[2] Wang T,Liu Y,Vasilakos A V.Survey on channel reciprocity based key establishment techniques for wireless systems[J].Wireless Networks,2015,21(6):1835-1846
[3] Goldsmith A.Wireless communications[M].New York:Cambridge University Press,2005
[4] 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 Guyue,YU Jiabao,HU Aiqun.Research on physical-layer security based on device and channel characteristics[J].Journal of Cryptologic Research,2020,7(2):224-248
[5] Shannon C E.Communication theory of secrecy systems[J].The Bell System Technical Journal,1949,28(4):656-715
[6] Furqan H M,Hamamreh J M,Arslan H.New physical layer key generation dimensions:subcarrier indices/positions-based key generation[J].IEEE Communications Letters,2021,25(1):59-63
[7] Yaacoub E.On secret key generation with massive MIMO antennas using time-frequency-space dimensions[C]//2016 IEEE Middle East Conference on Antennas and Propagation (MECAP).September 20-22,2016,Beirut,Lebanon.IEEE,2016:1-4
[8] Shimizu T,Iwai H,Sasaoka H.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] Mangang R K,Jagadeesh H.Do not forget the past:a buffer-aided framework for relay based key generation[J].Journal of Communications and Networks,2022,24(1):1-16
[10] Thai C D T,Lee J,Quek T Q S.Physical-layer secret key generation with colluding untrusted relays[J].IEEE Transactions on Wireless Communications,2016,15(2):1517-1530
[11] 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 Yinuo,JIN Liang,HUANG Kaizhi,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
[12] Lu T Y,Chen L Q,Zhang J Q,et al.Reconfigurable intelligent surface assisted secret key generation in quasi-static environments[J].IEEE Communications Letters,2022,26(2):244-248
[13] 陈发堂,郑金贵,陈峰,等.基于PID控制的自适应密钥生成[J].南京邮电大学学报(自然科学版),2023,43(3):11-18
CHEN Fatang,ZHENG Jingui,CHEN Feng,et al.Adaptive key generation based on PID control[J].Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition),2023,43(3):11-18
[14] Aldaghri N,Mahdavifar H.Physical layer secret key generation in static environments[J].IEEE Transactions on Information Forensics and Security,2020,15:2692-2705
[15] Hu L,Chen Y,Li G Y,et al.Exploiting artificial randomness for fast secret key generation in quasi-static environments[C]//2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP).October 22-24,2021,Nanjing,China.IEEE,2022:985-989
[16] Tang J,Wen H,Song H H,et al.Sharing secrets via wireless broadcasting:a new efficient physical layer group secret key generation for multiple IoT devices[J].IEEE Internet of Things Journal,2022,9(16):15228-15239
[17] Wang D,Chen F,Chen Y T,et al.Scramble-based secret key generation algorithm in physical layer security[J].Mobile Information Systems,2022,2022:1-9
[18] Li G Y,Yang H Y,Zhang J Q,et al.Fast and secure key generation with channel obfuscation in slowly varying environments[C]//IEEE Conference on Computer Communications.May 2-5,2022,London,United Kingdom.IEEE,2022:1-10
[19] Juels A,Wattenberg M.A fuzzy commitment scheme[C]//Proceedings of the 6th ACM Conference on Computer and Communications Security.New York,NY,USA:ACM,1999:28-36
[20] 3GPP.Evolved universal terrestrial radio access (EUTRA):physical channel and modulation (release 8)[S].TS36.211,2008
[21] Bellare M,Tessaro S,Vardy A.Semantic security for the wiretap channel[M]//Safavi-Naini R,Canetti R.Lecture Notes in Computer Science.Berlin,Heidelberg:Springer Berlin Heidelberg,2012:294-311
[22] Cover T M,Thomas J A.Elements of information theory[M].Hoboken,NJ,USA:John Wiley & Sons,2012
[23] Scarlett J,Cevher V.An introductory guide to Fano's inequality with applications in statistical estimation[J].arXiv e-Print,2019,arXiv:1901.00555
[24] Rukhin A,Soto J,Nechvatal J,et al.A statistical test suite for random and pseudorandom number generators for cryptographic applications[R].National Institute of Standards and Technology Special Publication 800-22,2001
[25] Liu H B,Wang Y,Yang J,et al.Fast and practical secret key extraction by exploiting channel response[C]//2013 Proceedings IEEE INFOCOM.April 14-19,2013,Turin,Italy.IEEE,2013:3048-3056
[26] Cho Y S,Kim J,Yang W Y,et al.MIMO-OFDM wireless communications with MATLAB[M].Hoboken,NJ,USA:John Wiley & Sons,2010

Backtracking scrambled key generation in quasi-static environment

WANG Dan[1] FANG Lei[1] HE Bin[1] CHEN Fatang[1]
1 School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract Physical layer security techniques utilize the wireless channel environment to dynamically generate keys, however, in quasi-static environment, slow channel transformation leads to insufficient key randomness and security. Here, a Backtracking Scrambled Key Generation (BSKG) algorithm is proposed. First, the real and imaginary parts of the channel coefficients are split and quantized to generate a longer key, which is reconciled, then the sum of the inconsistent indexes between the current key and previous key is used to generate a scrambling code to scramble the current key. Simulation shows that, compared with the existing multi-dimensional information and artificial randomness key generation method, the proposed algorithm has higher key generation rate and security, and the key leakage rate is close to 0.5 with the increase of the one-time pad key generation times, even if more relevant channel coefficients have been eavesdropped. The upper bounds on the probability of successful eavesdropping and their variations with the number of key generation N for general and bad channel conditions are estimated using semantic security and information-theoretic inequalities, respectively, when giving certain parameters, the upper bounds for these two cases turn out to be 2^{-77N} and 2^{-23N}.

Key words physical layer security; one-time pad; quasi-static environments; backtracking scrambled