

基于接收信号的多用户密钥生成方案

蔡奥林, 金梁, 钟州, 楼洋明

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 基于信道特征生成密钥的方案为通信安全带来了新思路。但在多用户慢衰落条件下, 基于信道特征的密钥生成方案由于参数变化慢, 导致密钥更新慢。针对此问题, 提出了基于接收信号的多用户密钥生成方案, 即通过块对角化预编码实现多个随机信号流的分发, 使基站与用户能够从用户接收信号中提取密钥。仿真结果表明, 提出的基于接收信号的多用户密钥生成方案能够有效提高多用户在准静态及慢衰落条件下的密钥速率。

关键词: 密钥生成; MISO; 多用户; 接收信号

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018082

Multuser secret key generation based on received signal

CAI Aolin, JIN Liang, ZHONG Zhou, LOU Yangming

National Digital Switching System Engineering & Technological R&D Center, Zhangzhou 450002, China

Abstract: The secret key generation method based on channel characteristic provides a new way for communication security. But under the conditions of multiuser and slow fading, because of the slow channel parameter changing rate, using the secret key generation method above can result in a low secret key rate. To solve this problem, a multiuser secret key generation method based on the received signal was proposed. By distributing the random signals to different users using block diagonalization precoding, base station and user can extract the secret key from the received signal. The novel method could significantly increase the secret key rate of multiuser under the quasi-static channel and slow-fading channel, which is verified by simulations.

Key words: secret key generation, MISO, multiuser, received signal

1 引言

在现有的通信系统中, 不仅合法接收方可以接收到无线通信信号, 由于其广播特性, 窃听方也可以接收到无线通信信号。因此, 无线通信信号的广播特性对通信安全造成了严重的威胁。

物联网作为第5代移动通信标准制定中的

重要应用场景, 目前正逐步广泛地应用于普通人的生活之中。物联网场景需求下, 要求大量的物联网节点具有小体积、低功耗的特点。目前, 针对物联网的安全研究多沿用传统的安全体制, 为了保障通信的安全需求, 通常在无线网络的高层利用复杂的加密算法和密钥分发来实现安全。而物联网节点所具有的小体积、低功耗、大数量的特点, 将增加密钥加密与分发

收稿日期: 2018-08-08; 修回日期: 2018-09-25

通信作者: 蔡奥林, alcai@stu.xidian.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61601514)

Foundation Item: The National Natural Science Foundation of China (No.61601514)

的实施难度。

而物理层安全中基于信道特征的密钥生成,为保障无线通信安全提供了新的思路,逐渐成为物理层安全的研究热点^[1-2]。无线信道具有时变性、互易性的特点,且窃听者在 2 个相干波长以外,其信道基本与合法信道不相干。合法通信用户可以从无线信道提取密钥。而无线信道的互易性,可以使生成的密钥免于分发,且实现复杂度较低。

文献[3-4]利用有噪观测值提取密钥,为物理层密钥提取提供了基础理论。在此基础上,基于各种信道特征参数的密钥生成方案先后出现。

然而,物理层信道参数的变化快慢很大程度上影响了物理层密钥的生成速率。所以,如果信道参数变化过慢,密钥的生成速率也会很低。例如,智能家居和智能水表等物联网设备一般情况下是固定不动的,导致设备周围的无线信道参数变化十分缓慢。这时密钥更新速度较慢,会严重威胁到用户的通信安全。

目前,已经有文献针对准静态信道场景存在的以上问题进行研究。文献[5]提出利用随机波束成形来模拟信道的波动变化,以弥补信道变化的不足。这就增加了密钥源的随机性,提升了密钥容量。文献[6]针对多天线系统,为了增加信道的随机性,随机改变各个天线上的幅度和相位来模拟信道的波动变化。同时,还有部分研究通过引入节点协作提高密钥速率。文献[7-8]通过协作节点的干扰来增加等效信道的随机性。文献[9-11]通过增加中继节点的数目来增加信道的数目,从而提高密钥容量。但协作的方案由于需要大量节点协作,难以在资源受限的物联网中实现^[12]。

由于上下行信道具有互易性,发送方可以利用信道参数和发送信号求得接收方的接收信号。此时通信双方可以将接收方的接收信号作为共享的密钥源。在这种接收信号作为共享随机源的场景下,当信道变化过慢时,可以利用人工可控的变量来增加提取密钥随机源的随机性。例如,文献[13]针对准静态变化的信道,通过发送随机变化的信号,增加接收信号的随机性,从而提升系统的密钥容量。

目前,针对多用户慢衰落场景,由于信道参数的变化过慢,且多个用户轮流与基站互发导频所用时间过长,因此还没有高速有效的密钥生成方案。按照传统的密钥生成方法,基站与一个用户互相发送一次导频只能和一个用户生成密钥。为了节省时隙资源,提高效率,本文提出一种多用户下的密钥生成方案,通过同时发送多流随机信号,同时与多个用户生成密钥。

2 基于发送多流随机信号的密钥生成原理

在该系统模型中,基站 Alice 有多根发送天线,天线数为 N_a ,有 N 个终端 Bob 与 K 个窃听者 Eve,所有合法用户都是单天线接收。每个窃听者 Eve_{*i*} 都被动窃听,每个终端 Bob_{*i*} 发送导频, Alice 对合法信道进行估计,生成 N 个随机信号,并对其进行预编码,然后将信号发送出去,各用户从接收信号中提取密钥,而基站利用信道信息估计各用户的接收信号,并从估计的信号中提取密钥。

为了将多个随机信号流发送给各用户,可以使用迫零波束赋型方案,如果使用迫零波束赋型作为多用户预编码方案对随机信号流进行预编码,则预编码与每个用户的信道组成的等效信道都是单位阵,不再包含信道信息。为了增加接收信号的随机性,充分利用信道的随机性,本文采用块对角化预编码。

如图 1 所示,系统模型中存在一个基站和多个用户,同时还存在配备多天线的窃听者。假设 Alice 与用户 Bob_{*i*} 间的信道衰落系数为 $h_{r,i} \in \mathbb{C}^{1 \times N_a}$, Alice 与 Eve_{*i*} 间的信道衰落系数为 $h_{e,i} \in \mathbb{C}^{N_E \times N_a}$ 。

用户 Bob_{*i*} 对其他用户的干扰矩阵为

$$\tilde{H}_i = \begin{bmatrix} h_{r,1}^T & \cdots & h_{r,i-1}^T & h_{r,i+1}^T & \cdots & h_{r,N}^T \end{bmatrix}^T \quad (1)$$

式(1)中, T 为矩阵转置符号。为避免发给用户 Bob_{*i*} 的随机信号流影响其他用户,其预编码矩阵需要在其他用户的零空间内,可以对干扰矩阵进行奇异值分解获得零空间矩阵。

$$\tilde{H}_i = [\tilde{U}_i U_i] \begin{bmatrix} \Sigma_i & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_i^H \\ \tilde{V}_i^H \end{bmatrix} \quad (2)$$

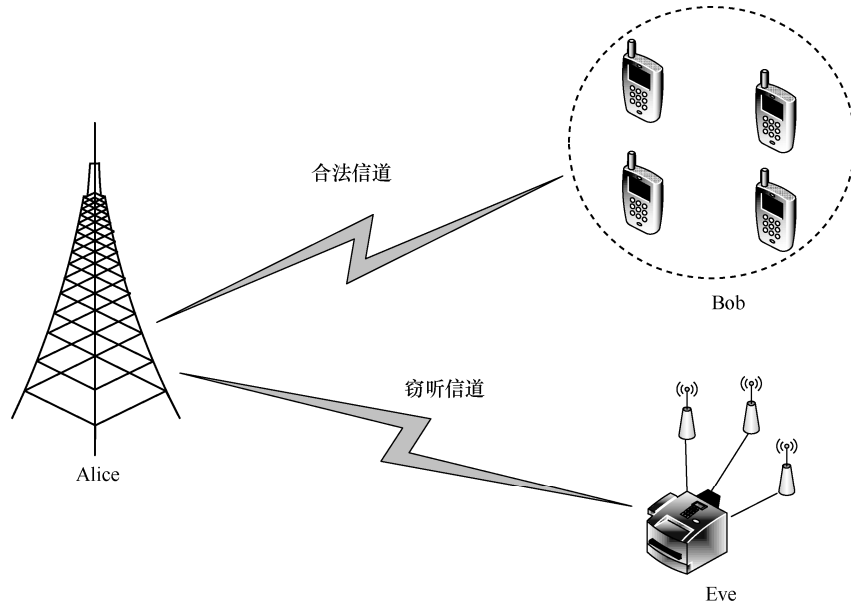


图1 系统模型

式(2)中, $\tilde{U}_i$ 是左酉矩阵的截尾矩阵, U_i 是左酉矩阵的非截尾矩阵, Σ_i 是奇异值矩阵, V_i^H 是右酉矩阵的截尾矩阵, $\tilde{V}_i^H$ 是右酉矩阵的非截尾矩阵。由于 $\tilde{V}_i$ 的列矢量是 $\tilde{H}_i$ 零空间的一组基组合, 假设 $\tilde{V}_i$ 作为预编码矩阵, 则等效矩阵为

$$\bar{H}_i = h_{r,i} \tilde{V}_i \quad (3)$$

对等效矩阵进行奇异值分解。

$$\bar{H}_i = [\bar{U}_i^1 \bar{U}_i^0] \begin{bmatrix} \Sigma_i & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} (\bar{V}_i^1)^H \\ (\bar{V}_i^0)^H \end{bmatrix} \quad (4)$$

式(4)中, $\bar{U}_i^1$ 是左酉矩阵的截尾矩阵, $\bar{U}_i^0$ 是左酉矩阵的非截尾矩阵, Σ_i 是奇异值矩阵, $(\bar{V}_i^1)^H$ 是右酉矩阵的截尾矩阵, $(\bar{V}_i^0)^H$ 是右酉矩阵的非截尾矩阵。对等效信道, 使用预编码 $\bar{V}_i^1$, 则对实际信道的预编码矩阵可以表示为

$$T_i = \tilde{V}_i^1 \bar{V}_i^1 \quad (5)$$

可以看到, 式(5)中的预编码矩阵并没有影响到式(2)和式(4)中的奇异值 Σ_i , 因此, 接收信号中包含奇异值 Σ_i 的信息, 即包含信道的部分参数信息。

Bob_i 与 Eve_i 的接收信号为

$$y_i = h_{r,i} T_i x_i + n_{r,i} \quad (6)$$

$$z_i = h_{e,i} T_i x_i + \sum_{l \neq i}^n h_{e,i} T_l x_l + n_{e,i} \quad (7)$$

其中, $n_{e,i}$ 是窃听者的接收噪声, $n_{r,i}$ 是终端的接收噪声, 噪声值都服从复高斯分布。 x_i 为 Alice 向 Bob_i 发送的随机信号。

3 密钥生成方案及性能分析

3.1 密钥提取流程

以下为多用户密钥生成方案提取密钥的流程。

1) 用户 Bob_i 轮流向基站发送双方已知的导频信号, 基站与各个用户之间的信道 $h_{r,i}$ 可以通过导频信号估算得到, 基站利用式(1)~式(4)生成预编码矩阵。

$$T_i = \tilde{V}_i^1 \bar{V}_i^1 \quad (8)$$

2) 基站生成随机信号矢量 $\mathbf{x}$, 使用块对角化预编码后发送给各个用户, 针对用户 Bob_i, 根据信道信息 $h_{r,i}$ 可以计算出接收信号矢量。

$$\hat{y}_i = h_{r,i} T_i x_i \quad (9)$$

3) 基站对计算出的接收信号矢量量化生成

密钥。

$$\hat{K} = Q(\hat{y}_i) \quad (10)$$

其中, $Q(\cdot)$ 为量化函数, 由量化的门限决定。 $\hat{K}$ 为基站生成的保密序列。

4) 用户 Bob_i 对接收信号 y_i 量化生成保密序列。

$$K = Q(y_i) \quad (11)$$

这里, K 为用户 Bob_i 生成的保密序列。

5) 基站与用户进行密钥协商并对保密序列隐私放大, 生成共享一致的密钥。

3.2 性能分析

3.2.1 可达密钥速率分析

由文献[2]可知, 可以用可达密钥速率来衡量系统模型的安全性, 而此系统模型单个用户的密钥速率可以表示为

$$R_{s,i} = \frac{1}{T_0} I(X_i; Y_i | Z_i) \geq 0 \quad (12)$$

这里, $I(X_i; Y_i | Z_i)$ 表示在窃听者观察到随机变量 Z_i 的条件下, 合法通信双方仍能够从随机量 X_i 、 Y_i 中提取出的密钥比特数。 T_0 表示一个密钥提取流程所需花费的时间。针对 3.1 节中的密钥提取流程, 可以计算用户 Bob_i 与基站 Alice 间生成共同密钥的密钥速率 $R_{s,i}$ 。

基站 Alice 针对 Bob_i 计算出其采样信号 $\hat{y}_i = h_{r,i} T_i x_i$, 用户 Bob_i 对接收信号采样得到 $y_i = \hat{y}_i + n_{r,i}$, 窃听者 Eve_i 根据窃听信号采样得到 $z_i = \hat{h}_{e,i} x_i + \sum_{l \neq i} h_{e,l} T_l x_l + n_{e,i}$, 其中, $\hat{h}_{e,i} = h_{e,i} T_i$, $n_{r,i}$ 为 Bob_i 的接收噪声, $n_{e,i}$ 为 Eve_i 天线上的接收噪声, 假设噪声均服从零均值复高斯分布。本模型的密钥容量计算如下。

$$\begin{aligned} C_{s,i} &= I(\hat{y}_i; y_i | z_i) \\ &= h(y_i | z_i) - h(y_i | \hat{y}_i, z_i) \\ &= h(y_i, z_i) - h(z_i) - h(n_{r,i}) \end{aligned} \quad (13)$$

其中, y_i 与 z_i 的联合熵为

$$h(y_i, z_i) = \log(\pi e)^{1+N_e} \left| E \begin{bmatrix} y_i y_i^H & y_i z_i^H \\ z_i y_i^H & z_i z_i^H \end{bmatrix} \right| \quad (14)$$

z_i 和 $n_{r,i}$ 的熵如下。

$$h(z_i) = \log(\pi e)^{N_e} \left| E [z_i z_i^H] \right| \quad (15)$$

$$h(n_{r,i}) = \log(\pi e) \quad (16)$$

式(16)中, N_e 是窃听者配备的天线数目。

$$\begin{aligned} C_{s,i} &= I(\hat{y}_i; y_i | z_i) \\ &= h(\hat{y}_i | z_i) - h(y_i | \hat{y}_i, z_i) \\ &= \log(\pi e)^{1+N_e} \left| E \begin{bmatrix} y_i y_i^H & y_i z_i^H \\ z_i y_i^H & z_i z_i^H \end{bmatrix} \right| \\ &\quad - \log(\pi e)^{N_e} \left| E [z_i z_i^H] \right| - \log(\pi e) \\ &= \log \left| p_i \|h_{r,i}\|^2 + 1 - p_i^2 \|h_{r,i}\|^2 \hat{h}_{e,i}^H \left(p_i \sum_{l=1}^n h_{e,l} T_l T_l^H h_{e,l}^H + I \right)^{-1} \hat{h}_{e,i} \right| \end{aligned} \quad (17)$$

这里, p_i 是基站对用户 Bob_i 的发送信号功率。而多个用户的密钥容量可以表示为

$$C_s = \sum_{i=1}^N C_{s,i} \quad (18)$$

本文考虑系统最差的情况, 即对于某个用户, 假设第 k 个窃听者为最危险的窃听者条件下, 用户密钥容量最小的情况。

$$C_{s,i} = \min_k \{C_{i,k}\} \quad (19)$$

则所有用户的密钥容量之和表示为

$$C_s = \sum_{i=1}^N \min_k \{C_{i,k}\} \quad (20)$$

3.2.2 密钥协商安全性分析

基站与用户密钥协商过程中, 基站对 3.1 节中第 3) 步生成的部分保密序列利用纠错码计算出其校验序列, 然后将校验序列用第 3) 步中生成的保密序列余下部分与其进行模二加后进行信道编码再发送出去。接收方将接收到的信息信道解码, 然后利用解出的信息和自身保密序列执行与基站相反的操作解码得到一致的序列。由于校验序列是用保密序列模二加后发送出去, 因此窃听者不能得到校验序列的信息。具体的纠错码方案可以采用低密度奇偶校验码^[14-15]或者极化码^[16]实现。

3.2.3 方案复杂性及时效性分析

在密钥生成过程中, 基站只需要进行信道估计可。而用户只需要发送一次导频信号, 然后直接从接收信号中提取密钥, 而不像传统方案一样需要估计信道信息。所以该方案能够降低用户开销, 有利于硬件资源不够充足的用户

生成密钥。

假设上行发送一次导频信号与下行发送一次随机信号所用时间均为 T 。如果利用传统的方案,每个终端都需要利用一个时间间隙向基站发送导频信号,然后基站的每一根天线都需要一个时间间隙来发送一个导频信号给一个用户,整个密钥生成流程所需花费的总时间为 $(N_a + N)T$ 。利用本文所提方案,在多用户场景下,每个用户利用一个时间间隙给基站发送导频信号,而基站利用一个时间间隙给所有用户各发送一个随机信号,所需要的总时间为 $(N+1)T$ 。可见本文一次多用户的密钥生成流程耗费更少的时间。

4 仿真分析

仿真内容如下:1) 在准静态信道条件下,平均总密钥速率随发送信号总功率的变化曲线;2) 在准静态信道条件下,平均总密钥速率随发送天线数目的变化曲线;3) 在慢衰落信道条件下,平均总密钥速率随发送信号总功率的变化曲线。

在仿真实验中,共有3个用户,每个用户都有3个窃听者。基站配备多天线,每个用户配备单天线,窃听者配备3天线。合法信道参数与窃听信道参数相互独立,且都服从复高斯分布。噪声功率设置为0 dBm。

在仿真中随机生成10 000组信道参数,并使文献[17]中所提出的 copula 熵对随机变量间的互信息进行估计。发送信号总功率单位为 dBm,总密钥速率单位 bit/T。

4.1 准静态衰落信道

在准静态状态下,信道的参数是保持不变的,因此相干时间 T_c 可以看成是趋近于无穷大的。信道参数的分布依然服从复高斯分布。图2中基站有8根发送天线,信噪比逐渐增加。图3中信噪比固定为5 dBm,噪声为0 dBm,发送天线数目逐渐增加。在传统的密钥生成方案中,基站与用户分别发送固定不变的导频信号,然后分别从各自的接收信号中提取密钥。但是,在准静态的环境下,信道的参数基本不变,基站与用户各自接收到的信号也几乎不变。本文利用接收信号来提取密钥,通过引入人工的随机变量,增加了接收信号的随机性,从而增加了平均总密钥速率。

图2分析了传统的密钥生成方案与本文所提密钥生成方案的平均总密钥速率。从图2中可以看出,本文所提方法有较高的平均总密钥速率。随着发送信号的功率增加,用户接收信号与基站估计信号的相关性受噪声的影响越来越小,因此平均总密钥速率逐渐增加。

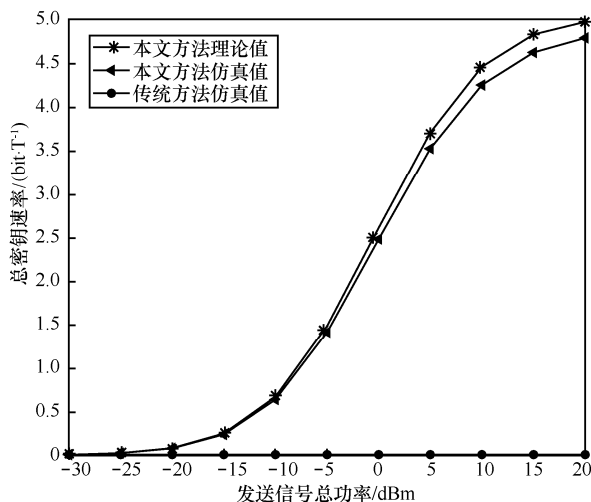


图2 准静态信道下平均总密钥速率随发送信号总功率变化

图3分析了本文所提方案平均总密钥速率随发送方天线数目的变化。在同等信噪比下,增加发送天线的数目将增加接收信号功率,接收信号的信噪比增加,平均总密钥速率随之增大。而传统的方案由于信道参数在整个密钥生成过程中几乎保持不变,因此平均总密钥速率几乎为零。

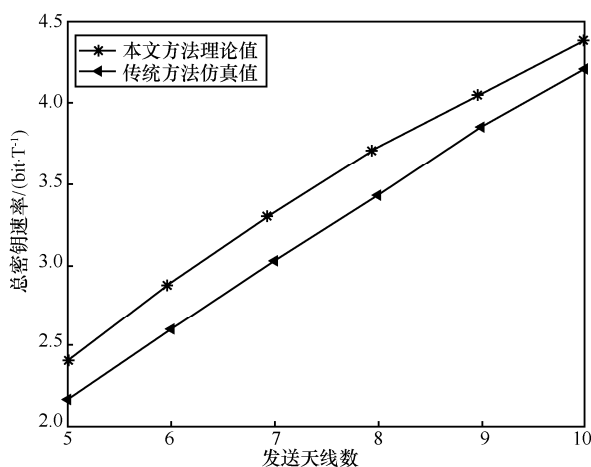


图3 准静态信道下平均总密钥速率随发送方天线数变化

4.2 慢衰落信道

慢衰落信道条件下,发送方天线设置为8,接收方为单天线。

图4分析对比了传统方案和本文方案的平均总密钥速率。在信道为慢衰落时，传统方案可以利用信道随机性提取密钥，而本文方案引入随机信号源增加了密钥提取源的随机性。且在传统方案中，基站的天线需要轮流向用户发送导频信号以供用户估计信道参数，而本文方案并不需要向用户发送导频以估计信道参数，而只需要基站向用户发送一次随机信号即可。

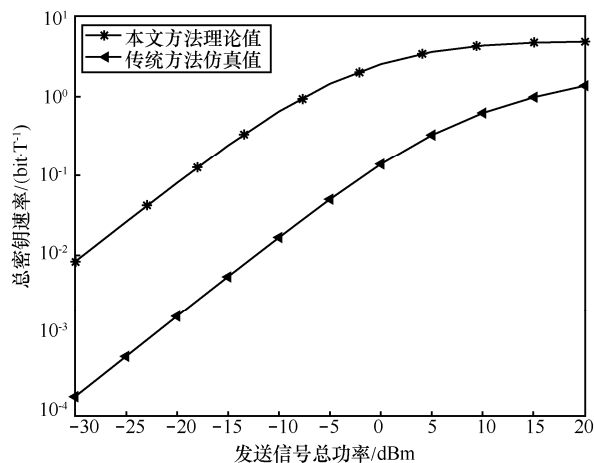


图4 慢衰落下平均总密钥速率随发送信号总功率变化

在传统方案中，随着发送信号功率增强，双方对信道参数估计的一致性也逐渐增大，因此平均总密钥速率得到提升。在本文方案中，由于发送信号的功率增加，基站估计信号与用户接收信号的相关性增加，平均总密钥速率得到提升。本文方案在引入发送信号和信道的随机性来增加密钥随机性的同时，利用块对角化预编码生成密钥过程所用时隙较少，所以本文方案能够获得更高的平均总密钥速率。

5 结束语

本文讨论了基于接收信号的多用户密钥生成方案。在信道变化缓慢的条件下，利用传统方案为多个用户生成密钥的速率较低，效率低。本文通过使用块对角化预编码方案，同时为多个用户提供随机信号流，提高用户接收信号的随机性，并让基站与用户从用户对应的接收信号中提取密钥。仿真表明，本文方案在多用户的准静态衰落场景下，可以通过同时为多个用户提供随机信号流，增加用户接收信号的随机性，有效提高密钥生成速率。

本文针对的是 TDD 下的密钥生成方案，在 FDD 场景下，由于信道失去了互易性，因此用户需要通过将信道信息发送给基站，为估计用户接收信号提供条件，而这样增加了信道信息泄露的风险。因此，FDD 场景下有效的密钥生成方案也是目前所亟待研究的方向。

参考文献：

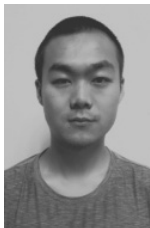
- [1] LIU Y, CHEN H H, WANG L. Physical layer security for next generation wireless networks: theories, technologies, and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 347-376.
- [2] ZHANG J, DUONG T Q, MARSHALL A, et al. Key generation from wireless channels: a review[J]. IEEE Access, 2017, 4(3): 614-626.
- [3] MAURER U M. Secret key agreement by public discussion from common information[J]. Information Theory IEEE Transactions on, 1993, 39(3): 733-742.
- [4] AHLWEDE R, CSISZAR I. Common randomness in information theory and cryptography. II. CR capacity[J]. Information Theory IEEE Transactions on, 1998, 44(1): 225-240.
- [5] MADISEH M G, NEVILLE S W, MCGUIRE M L. 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.
- [6] HUANG P, WANG X. Fast secret key generation in static wireless networks: a virtual channel approach[C]//INFOCOM. 2013: 2292-2300.
- [7] CHEN D, QIN Z, MAO X, et al. SmokeGrenade: an efficient key generation protocol with artificial interference[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(11): 1731-1745.
- [8] GOLLAKOTA S, KATABI D. Physical layer wireless security made fast and channel independent[C]//INFOCOM, 2011: 1125-1133.
- [9] CSISZAR I, NARAYAN P. Common randomness and secret key generation with a helper[C]//IEEE International Symposium on Information Theory. 2000: 157.
- [10] SHIMIZU T, IWAI H, SASAOKA H. Physical-layer secret key agreement in two-way wireless relaying systems[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3): 650-660.
- [11] LAI L, LIANG Y, DU W. cooperative key generation in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(8): 1578-1588.
- [12] MUKHERJEE A. Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints[J]. Proceedings of the IEEE, 2015, 103(10): 1747-1761.
- [13] 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: 信息科学, 2017(3).

LOU Y M, JIN L, ZHONG Z, et al. Secret key generation scheme

based on MIMO received signal spaces[J]. SCIENTIA SINICA Informationis, 2017(3).

- [14] CHAN W W, TAN F W, SHEA J M. Secret-sharing LDPC codes for the BPSK-constrained gaussian wiretap channel[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3): 551-564.
- [15] BLOCH M, BARROS J, RODRIGUES M R D, et al. Wireless Information-Theoretic Security-Part II: Practical Implementation[J]. IEEE Transactions on Information Theory, 2006, 54(6): 2515-2534.
- [16] ZHANG S, JIN L, LOU Y, et al. Secret key generation based on two-way randomness for TDD-SISO system[J]. China Communications, 2018, 15(7): 202-216.
- [17] ZENG X, DURRANI T S. Estimation of mutual information using copula density function[J]. Electronics Letters, 2011, 47(8): 493-494.

[作者简介]



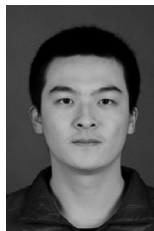
蔡奥林（1994-），男，河南偃师人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为物理层安全、无线通信安全。



金梁（1969-），男，北京人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为物理层安全、通信信号处理和阵列信号处理。



钟州（1982-），男，吉林公主岭人，国家数字交换系统工程技术研究中心讲师，主要研究方向为物理层安全。



楼洋明（1991-）男，浙江义乌人，国家数字交换系统工程技术研究中心研究实习员，主要研究方向为物理层安全。