中国科学: 信息科学 2017 年 第 47 卷 第 3 期: 362–373
SCIENTIA SINICA Informationis
论文

基于 MIMO 接收信号空间的密钥生成方案

楼洋明, 金梁*, 钟州, 黄开枝, 张胜军

国家数字交换系统工程技术研究中心, 郑州 450002
* 通信作者. E-mail: liangjin@263.net

收稿日期: 2016–05–16; 接受日期: 2016–06–28; 网络出版日期: 2016–11–30
国家自然科学基金 (批准号: 61521003)、国家高技术研究发展计划 (863 计划) (批准号: 2015AA01A708) 和中国博士后科学基金资助项目

摘要 针对现有密钥生成依赖信道参数, 在信道慢变条件下, 密钥生成速率不高的问题, 提出一种基于 MIMO 系统接收信号空间的密钥生成模型. 合法通信双方在当前接收信号空间中提取密钥, 并通过控制发送信号的变化来提高接收信号的随机性, 从而使密钥速率不受制于信道变化速度. 在此基础上, 提出一种密钥生成方法, 使合法通信双方可以获取接收信号空间并从中随机选择相同的接收信号矢量, 进而提取密钥. 同时使用迭代优化的方式获得最佳的发射功率分配方式, 使密钥速率最大. 仿真结果表明了该密钥生成方法的有效性.

关键词 物理层安全, 密钥生成, MIMO 系统, 接收信号空间, 功率分配

1 引言

随着无线通信技术的发展, 人们对于通信安全问题的关注程度越来越高. 未来无线网络场景中, 物联网、传感器网络的出现给通信安全带来了新的挑战. 在这些网络中, 终端往往具有体积小、功耗低的特点, 而采用传统的加密方式往往需要复杂的计算过程, 消耗大量的计算资源, 因此需要采取更加合适的轻量级加密方法.

无线通信与有线通信不同, 由于没有有线介质的束缚, 对于不同目的节点来说, 在无线信号到达的过程中, 往往会经历不同“路径”. 而这些“路径”的叠加往往具有很强的随机性, 是一种天然的随机源. 因此, 无线信道是一种天然的密钥源. 对于合法的无线通信双方来说, 已有研究表明, 其上下行信道相同, 且在相干时间内可认为信道参数不变, 合法通信双方可以通过信道估计获得两者之间的信道参数 [1], 因此合法通信双方间的无线信道又具有可测性. 这为从无线信道中提取密钥提供了可能.

Maurer 首先在文献 [2] 中提出了一种利用共享随机信息进行密钥生成的方法, 该方法的关键在于如何在合法通信双方间共享随机信息, 即如何确定合法通信双方独有的随机源. Ahlswede 和 Csiszar 在文献 [3] 中给出了有噪条件下密钥生成的基本模型, 合法通信双方及窃听者均从同一个随机源中获

引用格式: 楼洋明, 金梁, 钟州, 等. 基于 MIMO 接收信号空间的密钥生成方案. 中国科学: 信息科学, 2017, 47: 362–373, doi: 10.1360/N112016-00001
Lou Y M, Jin L, Zhong Z, et al. Secret key generation scheme based on MIMO received signal spaces (in Chinese). Sci Sin Inform, 2017, 47: 362–373, doi: 10.1360/N112016-00001

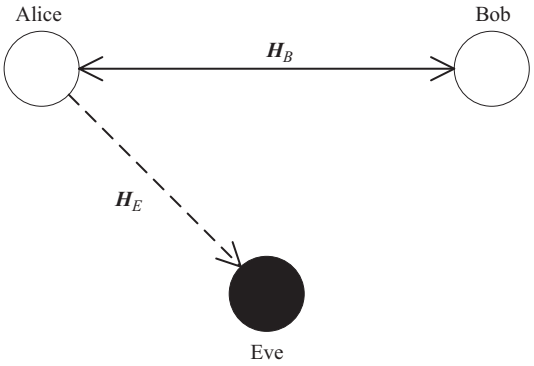


图 1 系统模型

Figure 1 System model

得信息, 而合法通信双方可利用两者间存在的反馈信道通信从而使获得的信息趋于一致. 以上述思想为基础, 近年来对于如何利用无线信道特征进行密钥生成的研究越来越多 [4~8], 利用信道的幅、频、相等特征作为密钥源来快速、准确地提取密钥. MIMO 技术作为一种空间复用技术, 通过在收发端配置多天线来产生大量的并行信道, 产生大量可以用于密钥提取的信道信息, 仅仅通过增加天线数量就能够极大地提高密钥生成的速率, 因此在密钥生成领域受到广泛关注 [9~11].

然而, 目前针对 MIMO 信道仅仅是简单地利用通过信道估计得来的信道信息, 即信道矩阵来提取密钥, 其密钥长度及更新完全依赖于自然信道的变化, 当信道变化较慢时, 难以在短时间内提取出足够长的密钥, 降低了安全性能.

其次, 在 MIMO 系统中, 若利用信道矩阵提取密钥, 通信双方均需要大量的信道估计运算及交互过程以获取所有信道信息, 当通信双方的天线资源及计算资源严重不对等时 (如 Massive MIMO 系统中, 基站与终端通信), 对处于资源劣势的终端来说, 信道估计的开销过大.

针对上述问题, 本文首先讨论了基于接收信号空间提取密钥的原理, 然后设计一种基于接收信号空间的密钥生成方案, 其主要思想在于: 接收信号可由发送信号与信道计算得出, 因此, 终端与基站可以从接收信号中提取相同的密钥; 且由于接收信号的随机特性来源于发送信号与信道, 相对于单独应用信道信息来说, 具有更好的随机特性, 可以取得更长的密钥. 在此基础上给出了针对该方案的优化功率分配方法, 并对方案在不同条件下的密钥速率, 即单位时间内提取的密钥长度进行了数值仿真.

2 基于 MIMO 接收信号空间密钥提取模型

2.1 系统模型

系统模型如图 1 所示, 合法的发送方 Alice 与接收方 Bob 希望能够利用两者间信道的互易性来共享随机信号, 从而进行密钥提取. Eve 为被动窃听者, 可以对 Alice 与 Bob 发送的任何信息进行窃听, 而不对密钥生成过程进行干扰. Alice, Bob, Eve 均配备多天线, 假设三者配备的天线数分别为 N_A, N_B 和 N_E, 天线间距大于半波长.

以 Bob 端的密钥提取过程为例. 假设 Alice 的发射信号 $\boldsymbol{X}$ 为 $N_A \times n$ 的矩阵, 由连续 n 个时刻的发送信号向量组成, Alice 与 Bob 间的信道为 $\boldsymbol{H}_B \in \mathbb{C}^{N_B \times N_A}$, Alice 与 Eve 间的信道为 $\boldsymbol{H}_E \in \mathbb{C}^{N_E \times N_A}$, 假设无线信道为块衰落, 则在整个密钥生成过程中信道参数保持不变. Bob 与 Eve 的接收信号如式 (1)

所示

$$\begin{aligned}\boldsymbol{Y}&=\boldsymbol{H}_B\boldsymbol{X}+\boldsymbol{W}_B,\\ \boldsymbol{Z}&=\boldsymbol{H}_E\boldsymbol{X}+\boldsymbol{W}_E,\end{aligned}\tag{1}$$

其中 $\boldsymbol{Y}$ 与 $\boldsymbol{Z}$ 分别为 Alice 与 Eve 的接收信号. $\boldsymbol{W}_B$ 与 $\boldsymbol{W}_E$ 为加性高斯白噪声矩阵, 且二者中的各元素均为服从 $\mathcal{CN}(0,1)$ 的独立随机变量.

2.2 常规物理层密钥生成方法

在一般密钥生成方法中, Bob 接收到 $\boldsymbol{Y}$ 后, 对其中的信道参数进行量化, 进而提取密钥. 之后由 Bob 发送信号, Alice 进行接收, 重复上述步骤即可在 Alice 端提取密钥. 一般认为, 上下行的无线信道具有互易性, 因此可认为相干时间内 Alice 与 Bob 间的上下行信道参数基本相同, 二者的接收信号具有极强的相关性. 之后再通过量化接收信号信息获得密钥比特, 交换协商信息提高密钥比特的一致性, 删除协商过程中泄露的密钥比特提高安全性等步骤, 得到最终密钥, 用来保障通信安全. 而对于窃听者 Eve 来说, 由于空间位置不同, 无法获取 Alice 与 Bob 间的信道信息, 难以得到正确的密钥. 可见, Alice 与 Bob 间的信道信息具有私有性, 可以作为一种私有随机源来进行密钥提取. 从式 (1) 中可以看出, 在整个通信过程中, Bob 用于密钥提取的资源来自于接收信号 $\boldsymbol{Y}$. 当发送信号 $\boldsymbol{X}$ 固定不变或通信双方已知时, 由于主信道 $\boldsymbol{H}_B$ 只与合法通信双方所处的位置有关, 且具有随机性, 因此由 $\boldsymbol{H}_B$ 来确保密钥私有并能够被随时更新. 但是在信道慢变的情况下, 仅利用 $\boldsymbol{H}_B$ 来生成密钥, 密钥速率将会大大降低.

2.3 基于接收信号空间的密钥生成模型

为了确保具有足够快的密钥更新速率, 可令发送信号矩阵 $\boldsymbol{X}$ 为随机变量. 假设 $\boldsymbol{X}$ 满秩, 接收信号 $\boldsymbol{Y}$ 可以写为如下形式:

$$\begin{aligned}\boldsymbol{Y}&=\boldsymbol{H}_B\boldsymbol{X}+\boldsymbol{W}_R\\ &=\left[\begin{array}{ccc}\boldsymbol{h}_1&\cdots&\boldsymbol{h}_{N_A}\end{array}\right]\left[\begin{array}{ccc}x_1^{(1)}&\cdots&x_1^{(n)}\\ \vdots&\ddots&\vdots\\ x_{N_A}^{(1)}&\cdots&x_{N_A}^{(n)}\end{array}\right]+\left[\begin{array}{ccc}\boldsymbol{w}_B^{(1)}&\cdots&\boldsymbol{w}_B^{(n)}\end{array}\right]\\ &=\left[\begin{array}{ccc}\sum\limits_{k=1}^{N_A}\boldsymbol{h}_k x_k^{(1)}+\boldsymbol{w}_B^{(1)}&\cdots&\sum\limits_{k=1}^{N_A}\boldsymbol{h}_k x_k^{(n)}+\boldsymbol{w}_B^{(n)}\end{array}\right],\end{aligned}\tag{2}$$

式 (2) 中, $\boldsymbol{h}_k$ 和 $x_k^{(t)}$ 分别为 $\boldsymbol{H}_B$ 的列向量以及在时刻 t, Alice 第 k 根天线上的发送信号, $\boldsymbol{w}_B^{(t)}$ 为时刻 t 的噪声向量. 从结果中可以看出, Bob 在任一时刻的接收信号向量, 均为信道矩阵 $\boldsymbol{H}_B$ 列向量的线性组合. 我们将 Bob 的所有接收信号构成的线性空间称为 Bob 的接收信号空间, 记作 V_B, 则 V_B 为信道矩阵 $\boldsymbol{H}_B$ 的列空间, 即

$$V_B=R(\boldsymbol{H}_B),\tag{3}$$

其中 $R(\cdot)$ 表示矩阵的值域. 选择 $\boldsymbol{H}_B$ 的列向量中的最大线性无关组构成 V_B 的一组基, 向量的个数为

V_B 的维数, 即 $\boldsymbol{H}_B$ 的秩, 记作 K. Bob 的接收信号可以重新写作如下形式:

$$\boldsymbol{Y}=\left[\begin{array}{ccc}\boldsymbol{h}_{m_1} & \cdots & \boldsymbol{h}_{m_K}\end{array}\right]\left[\begin{array}{ccc}x_1^{(1)} & \cdots & x_1^{(n)}\\ \vdots & \ddots & \vdots\\ x_{m_K}^{(1)} & \cdots & x_{m_K}^{(n)}\end{array}\right]+\left[\begin{array}{ccc}\boldsymbol{w}_B^{(1)} & \cdots & \boldsymbol{w}_B^{(n)}\end{array}\right], \tag{4}$$

其中 $[\,\boldsymbol{h}_{m_1}\ \cdots\ \boldsymbol{h}_{m_K}\,]$ 为 $\boldsymbol{H}_B$ 列向量的最大线性无关组. 在 MIMO 系统中, 接收信号空间为信道矩阵的列空间.

由上述分析可以看出, 信道矩阵只是接收信号空间的一组基, 而整个接收信号空间中的接收信号矢量是无穷的, 合法通信双方只要能够确定空间的基, 就能够选取相同的矢量从而生成密钥. 这样就能够扩大密钥空间, 增加能够提取的密钥数量.

若在一次相干时间内, 对信号接收空间内选取的样点不变, 即式 (2) 中的 $\boldsymbol{X}$ 保持不变时, 该式所描述的通信过程可以看作是一次信道估计过程, 在接收信号空间内选取的样点即为信道矩阵的列向量, 密钥的时变性由信道的时变性决定. 因此, 基于无线信道生成密钥的方法可以看作上述方法的一个特例.

假设发送信号向量为 $\boldsymbol{x}$, 各路发送信号相互独立, 且服从 $\mathcal{CN}\left(0,\sigma_i^2\right)$, 则发送信号的协方差矩阵为

$$\boldsymbol{K}_{\boldsymbol{xx}}=E\left[\boldsymbol{x}\boldsymbol{x}^{\mathrm{H}}\right]=\left[\begin{array}{ccc}\sigma_1^2 & & \\ & \ddots & \\ & & \sigma_{N_A}^2\end{array}\right], \tag{5}$$

其中 $E[\cdot]$ 表示期望. 在不考虑加性噪声的情况下, 接收信号 $\boldsymbol{y}$ 满足下式:

$$\boldsymbol{y}=\boldsymbol{H}_B\boldsymbol{x}=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{x}, \tag{6}$$

其中 $\boldsymbol{U}$, $\boldsymbol{\Sigma}$, $\boldsymbol{V}$ 分别为对 $\boldsymbol{H}_B$ 进行奇异值分解所得的左奇异矩阵、奇异值矩阵、右奇异矩阵. 则接收信号向量 $\boldsymbol{y}$ 的协方差矩阵为

$$\boldsymbol{K}_{\boldsymbol{yy}}=E\left[\boldsymbol{y}\boldsymbol{y}^{\mathrm{H}}\right]=E\left[\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{x}\boldsymbol{x}^{\mathrm{H}}\boldsymbol{V}\boldsymbol{\Sigma}\boldsymbol{U}^{\mathrm{H}}\right]=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{K}_{\boldsymbol{xx}}\boldsymbol{V}\boldsymbol{\Sigma}\boldsymbol{U}^{\mathrm{H}}, \tag{7}$$

易知 $\boldsymbol{U}\boldsymbol{\Sigma}^2\boldsymbol{U}^{\mathrm{H}}$ 正定.

若处理接收信号令 $\boldsymbol{r}=\boldsymbol{U}^{\mathrm{H}}\boldsymbol{y}$, 处理发送信号令 $\boldsymbol{s}=\boldsymbol{V}\boldsymbol{x}$, 则 $\boldsymbol{r}$ 的协方差矩阵为

$$\boldsymbol{K}_{\boldsymbol{rr}}=E\left[\boldsymbol{U}^{\mathrm{H}}\left(\boldsymbol{H}_B\boldsymbol{s}\boldsymbol{s}^{\mathrm{H}}\boldsymbol{H}_B^{\mathrm{H}}\right)\boldsymbol{U}\right]=\boldsymbol{\Sigma}\boldsymbol{K}_{\boldsymbol{xx}}\boldsymbol{\Sigma}. \tag{8}$$

综合上述分析, 我们能够得到以下结论:

结论 1: 接收信号空间 $V_B=R(\boldsymbol{H}_B)$, 由于 $R(\boldsymbol{H}_B)=R(\boldsymbol{U})$, 因此 $V_B=R(\boldsymbol{U})$, 即接收信号空间由 $\boldsymbol{U}$ 确定, 所有接收信号均为 $\boldsymbol{U}$ 各列的线性组合.

结论 2: 发送信号向量 $\boldsymbol{x}\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{K}_{\boldsymbol{xx}})$, 则接收信号向量 $\boldsymbol{y}\sim\mathcal{CN}\left(\boldsymbol{0},\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{K}_{\boldsymbol{xx}}\boldsymbol{V}\boldsymbol{\Sigma}\boldsymbol{U}^{\mathrm{H}}\right)$. 特别地, 采用 $\boldsymbol{U}^{\mathrm{H}}$ 处理接收信号,$\boldsymbol{V}$ 处理发送信号, 则处理后 $\boldsymbol{r}\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{\Sigma}\boldsymbol{K}_{\boldsymbol{xx}}\boldsymbol{\Sigma})$, 此时 $\boldsymbol{r}$ 的各元素的分布相互独立, 可以独立的用来提取密钥.

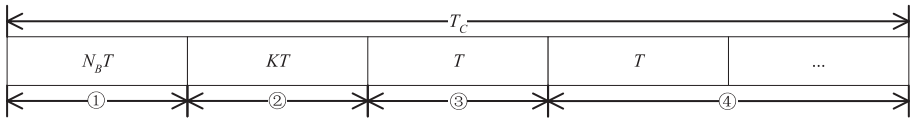


图 2　通信方案时间分配

Figure 2　Time allocation scheme

3　密钥提取方法

由上一节的分析可知, 用于密钥提取的信道参数均来自于接收信号空间, 通过从接收信号空间中选取接收信号矢量来生成密钥, 其密钥速率的提高就可以不受制于自然信道的变化速度. 相对于传统直接利用现有信道的信道参数来提取密钥的方法, 合法通信双方能够从接收信号空间中提取密钥, 其方法的关键在于: (1) 由天线数多的一方, 即中心站进行信道估计, 减少开销, 同时根据结论 1, 利用奇异值矩阵的正交性就能够使终端得到接收信号空间的基; (2) 利用发送信号的方法使合法通信双方从接收信号空间中选择相同的信号矢量, 并利用结论 2 确保从各天线的接收信号中提取的信号相互独立; (3) 整个通信过程由中心站主导, 各终端配合中心站完成密钥的提取过程, 导频由终端发送, 基站完成信道估计. 以此为基础, 本文提出下述密钥提取方案.

假设发送导频并估计信道所用时间为 T_P, 发送并处理一次发送信号矢量所用时间为 T, 整个通信过程即相干时间 T_C 内, 主信道的信道矩阵 $\boldsymbol{H}_B$ 不变. 具体密钥提取过程可按照如下方式进行:

① Alice 侧信道估计: Bob 在公共信道中发送导频序列, Alice 估计二者间的信道矩阵 $\boldsymbol{H}_B$, 秩为 K. 并对 $\boldsymbol{H}_B$ 做奇异值分解, 得到 $\boldsymbol{U}$, $\boldsymbol{\Sigma}$, $\boldsymbol{V}$.

$$\boldsymbol{H}_B = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}. \tag{9}$$

② Bob 侧信道参数提取: Alice 向 Bob 发送信号为 $\boldsymbol{V}_K$, 即 $\boldsymbol{V}$ 的前 K 列, 则 Bob 的接收信号为 $\boldsymbol{U}\boldsymbol{\Sigma}_K$, $\boldsymbol{\Sigma}_K$ 为 $\boldsymbol{H}_B$ 的非零奇异值矩阵. 由于 $\boldsymbol{U}$ 各列正交, $\boldsymbol{\Sigma}_K$ 为实对角阵, 所以易得到 $\boldsymbol{U}$ 和 $\boldsymbol{\Sigma}$.

$$\boldsymbol{y}_{B1} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{V}_K = \boldsymbol{U}\boldsymbol{\Sigma}_K. \tag{10}$$

③单次密钥提取: Alice 采用 $\boldsymbol{V}$ 作为发送矩阵, Bob 采用 $\boldsymbol{U}^{\mathrm{H}}$ 作为接收矩阵, Alice 的发送信号向量 $\boldsymbol{x} \sim \mathcal{CN}\left(\boldsymbol{0}, \sigma_i^2 \boldsymbol{I}\right)$, 则接收信号向量 $\boldsymbol{r} \sim \mathcal{CN}\left(\boldsymbol{0}, \boldsymbol{\Sigma}\boldsymbol{K}_{\boldsymbol{x}\boldsymbol{x}}\boldsymbol{\Sigma}\right)$, Alice 与 Bob 分别从 $\boldsymbol{\Sigma}\boldsymbol{x}$ 及 $\boldsymbol{r}$ 中提取密钥.

$$\boldsymbol{r} = \boldsymbol{U}^{\mathrm{H}}\boldsymbol{y}_{B2} = \boldsymbol{U}^{\mathrm{H}}\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{V}\boldsymbol{x} = \boldsymbol{\Sigma}\boldsymbol{x}. \tag{11}$$

④密钥组合与生成: 在整个相干时间 T_C 内重复步骤③, 直到获得足够长的密钥. 信道矩阵改变, 即超过信道相干时间后, 从步骤①重新开始.

从图 2 中可以看出, 采用上述方法提取接收信号空间来生成密钥, 耗费的通信时间为 $(N_B + K + n)T$, n 为步骤③的重复次数, 而通信双方估计整个信道矩阵, 耗费通信时间为 $(N_A + N_B)T$. 假设实际通信系统中 $N_A \gg N_B \geqslant K$, 即通信双方天线资源不对等时, 采用所提方法可以大大缩短耗费的通信时间, 且可以通过控制 n 来控制密钥的更新频率, 相对于传统方法更加方便灵活.

4 性能分析

4.1 安全性分析

合法通信双方在窃听者窃听到随机量 Z 的条件下, 分别从随机量 X、Y 中提取并进行协商, 最终得到安全密钥. 从单位符号中得到的最大密钥的长度被称为密钥容量. 由文献 [3] 可知, 密钥容量是衡量密钥生成方案性能的重要指标, 通常由条件互信息表示, 即

$$C_s = I\left(X;Y|Z\right) \geqslant 0, \tag{12}$$

因此, $C_s > 0$ 表示合法通信双方能够生成安全的密钥, 该密钥不会被窃听方获取. 在密钥容量不变的条件下, 单位时间内能够获取越多用于密钥生成的符号, 密钥速率就越高.

从互信息的定义易得到下式:

$$I\left(X;Y|Z\right) = h\left(X|Z\right) - h\left(X|Y,Z\right) = h\left(Y|Z\right) - h\left(Y|X,Z\right), \tag{13}$$

这表明, 以下情况发生时, 将无法生成安全密钥, 即 $C_s = 0$: ① X 与 Y 无关; ② Z 与 X 或 Y 完全相关. 针对第 3 节中提出的方法: 情况①表明 Alice 计算出的 Bob 接收信号与 Bob 实际的接收信号无关, 这只有在信噪比极低的情况下才会出现; 情况②表明 Eve 的能够完全通过接收的信号构造出 Bob 的接收信号 (包括接收噪声), 这就需要 Eve 与 Bob 处于同一物理位置, 且两者的接收噪声极大相关.

在第 3 节描述的密钥提取过程中, Alice 没有发送导频序列, 因此 Eve 无法得到窃听信道 $\boldsymbol{H}_E$ 和 Alice 的发送信号. 尽管 Alice 发送了 $\boldsymbol{V}_K$, Eve 可以接收到一部分有关 $\boldsymbol{H}_B$ 的信息, 但由于奇异值分解的结果不唯一, $\boldsymbol{V}_K$ 与 $\boldsymbol{H}_B$ 不存在一一对应关系, 因此 Eve 无法通过接收的信号构造出 Bob 的接收信号. 综上所述, 在信噪比不过低的条件下, 采用第 3 节方案所得的密钥容量 $C_s > 0$, 即在文中所提场景下, 该密钥生成方案是安全的.

如第 3 节所示，采用本文所提出的密钥提取方案, 首先需要 Alice 估计合法通信双方间的信道矩阵. 由于在信道估计过程中会受到噪声的影响, Alice 的信道估计值与实际的信道参数往往存在误差. 然而, 对于密钥生成技术来说, 为了能够协商出一致的密钥, 仅需要合法通信双方之间得到的信息强相关, 而不需要保证该信息与实际信道参数完全一致. 因此, 可以认为 Alice 的信道估计值是准确的, 并将信道估计的误差折算至接收端的接收噪声中, 从而简化本文所提出方案的密钥容量分析过程.

假设存在窃听者 Eve, 窃听信道矩阵为 $\boldsymbol{H}_E$, 接收噪声向量 $\boldsymbol{w}_B, \boldsymbol{w}_E \sim \mathcal{CN}\left(\boldsymbol{0}, \boldsymbol{I}\right)$. 在上述通信过程步骤③和④中, Alice 采用 $\boldsymbol{V}$ 作为发送矩阵, 发送随机信号向量为 $\boldsymbol{x}$, Bob 与 Eve 的接收信号向量分别为

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{H}_B\boldsymbol{V}\boldsymbol{x} + \boldsymbol{w}_B, \\ \boldsymbol{z} &= \boldsymbol{H}_E\boldsymbol{V}\boldsymbol{x} + \boldsymbol{w}_E. \end{aligned} \tag{14}$$

Bob 采用 $\boldsymbol{U}^{\mathrm{H}}$ 作为接收矩阵处理接收信号 $\boldsymbol{y}$, 处理结果 $\boldsymbol{r} = \boldsymbol{U}^{\mathrm{H}}\boldsymbol{y}$, $\boldsymbol{s}$ 为 Bob 对 $\boldsymbol{r}$ 的估计值, 记 $\hat{\boldsymbol{H}}_B = \boldsymbol{\Sigma}$, 则

$$\begin{aligned} \boldsymbol{s} &= \hat{\boldsymbol{H}}_B\boldsymbol{x}, \\ \boldsymbol{r} &= \hat{\boldsymbol{H}}_B\boldsymbol{x} + \hat{\boldsymbol{w}}_B. \end{aligned} \tag{15}$$

Alice 与 Bob 分别从 $\boldsymbol{s}$ 与 $\boldsymbol{r}$ 中提取密钥, $\hat{\boldsymbol{w}}_B = \boldsymbol{U}^{\mathrm{H}}\boldsymbol{w}_B$.

对于 Alice 与 Bob 来说, 步骤①和②结束后, 双方就得到了接收信号空间的基, 因此只要选取相同的坐标, 即发送信号矢量 $\boldsymbol{x}$, 就能够从同一接收信号空间中选取相同的接收信号矢量用以提取密钥.

在相干时间 T_C 内, 主信道 $\boldsymbol{H}_B$ 及窃听信道 $\boldsymbol{H}_E$ 可认为保持不变, 即信道为准静态 (quasi-static). 此时, 密钥容量可由下式表示:

$$C_s = \log\left|\boldsymbol{I} + \boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\right| - \log\left|\boldsymbol{I} + \boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\right| > 0, \tag{16}$$

其中, $\hat{\boldsymbol{H}}_E = \boldsymbol{H}_E\boldsymbol{V}$. 为方便描述, 本文中 $\log(\cdot)$ 均表示以 2 为底的对数. 详细推导参见附录 A.

4.2 方案性能优化

如果 Alice 能够获得自身与 Eve 间的 CSI, 当窃听方 Eve 的天线数少于发送方 Alice, 即窃听信道不满足列满秩条件时, 那么 Alice 就可以在窃听信道的零空间中发送信息, 此时 Eve 将无法窃听到任何信息, 密钥速率将随着信噪比地上升呈线性增长 [10].

文献 [8] 中给出了在高信噪比条件下 MIMO 系统的密钥容量, 并且可以证明在主信道矩阵与窃听信道矩阵均为列满秩的情况下, 随着信噪比地提高, 密钥容量总能够达到一个上界. 因此, 我们只需要考虑如何在信道固定的条件下, 通过改变发送信号的功率分配方式使当前信噪比条件下的密钥容量达到最大.

假设此时等效主信道矩阵 $\hat{\boldsymbol{H}}_B$ 与等效窃听信道矩阵 $\hat{\boldsymbol{H}}_E$ 均为列满秩, 则式 (16) 中所描述的密钥容量可以进一步变形如下:

$$\begin{aligned} C_s\left(\sigma_1^2, \sigma_2^2, ..., \sigma_{N_a}^2\right) = &\log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| \\ &- \log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| \\ &+ \log\frac{\left|\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right|}{\left|\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right|}, \end{aligned} \tag{17}$$

式 (17) 中最后一项为常数项. 令 $p_i = \sigma_i^2$, $\boldsymbol{p} = (p_1, p_2, ..., p_{N_A})^{\mathrm{T}}$, 即 $\boldsymbol{K}_{\boldsymbol{xx}}$ 对角线上元素组成的列向量. 令式 (17) 前两项之和为 $f(\boldsymbol{p})$. 则在总发射功率一定时, 最佳功率分配问题如下表示:

$$\begin{aligned} \max_{\boldsymbol{p}} \quad & f(\boldsymbol{p}) = \log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| - \log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right|, \\ \text{s.t.} \quad & p_i > 0, \quad \sum_i p_i = P, \end{aligned} \tag{18}$$

$f(\boldsymbol{p})$ 中的两项均为关于 $\left(\sigma_1^2, \sigma_2^2, ..., \sigma_{N_A}^2\right)$ 的凸函数, 但无法保证前两项之和依然为凸函数, 难以求解. 该问题与文献 [12] 中的优化问题类似, 为了解决该问题, 我们对 $f(\boldsymbol{p})$ 的第二项进行泰勒级数展开, 用展开式来近似表示, 从而求取式 (18) 的解. 首先利用一阶泰勒级数展开式来近似表示 $f(\boldsymbol{p})$. 对 $f(\boldsymbol{p})$ 的第二项在 $\tilde{\boldsymbol{p}}$ 处展开, 则有

$$\begin{aligned} f(\boldsymbol{p}) \simeq &\log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| - \log\left|\tilde{\boldsymbol{K}}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| \\ &- \frac{1}{\ln 2}\left[\mathrm{diag}\left(\left(\tilde{\boldsymbol{K}}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right)^{-1}\right)\right]^{\mathrm{T}}(\boldsymbol{p} - \tilde{\boldsymbol{p}}) \\ \triangleq &\ \tilde{f}(\boldsymbol{p}), \end{aligned} \tag{19}$$

表 1 密钥容量优化迭代算法

Table 1 Key capacity optimization iterative algorithm

1) Initialize $\tilde{\boldsymbol{p}}$. Set $\tilde{p}_i = P/N_A$;
2) Solve Eq.(20) and find the optimal solution $\boldsymbol{p}^*$;
3) Update $\tilde{\boldsymbol{p}} \leftarrow \boldsymbol{p}^*$;
4) Repeat Step 2 to Step 3 until $\tilde{\boldsymbol{p}}$ essentially unchanged.

推导详见附录 B, 此时优化问题变为

$$\begin{aligned} \max_{\boldsymbol{p}} \quad & \tilde{f}(\boldsymbol{p}) = \log\left|\boldsymbol{K}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B + \hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| - \log\left|\tilde{\boldsymbol{K}}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| \\ & - \frac{1}{\ln 2}\left[\mathrm{diag}\left(\left(\tilde{\boldsymbol{K}}_{\boldsymbol{xx}} + \left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right)^{-1}\right)\right]^{\mathrm{T}}(\boldsymbol{p} - \tilde{\boldsymbol{p}}), \qquad (20) \\ \text{s.t.} \quad & p_i > 0, \quad \sum_i p_i = P, \end{aligned}$$

其中 $\tilde{\boldsymbol{K}}_{\boldsymbol{xx}}$ 为 $\tilde{\boldsymbol{p}}$ 元素构成的对角阵, $diag(\cdot)$ 为矩阵主对角线上的元素组成的列向量. 由于一阶泰勒级数展开式为线性函数, 所以 $\tilde{f}(\boldsymbol{p})$ 为关于 $\boldsymbol{p}$ 的凸函数, 能够进行求解. 注意到, $\tilde{\boldsymbol{p}}$ 的选择将影响式 (19) 的优化求解结果, 且难以求得其闭式解, 因此可以为 $\tilde{\boldsymbol{p}}$ 选择合适的初始值, 并在每个迭代步骤中采用本次求得的最优解 $\boldsymbol{p}^*$ 更新 $\tilde{\boldsymbol{p}}$, 使式 (20) 所得的最优解逐渐逼近式 (19) 所得的最优解, 迭代具体步骤如表 1 所示, 收敛性证明见文献 [13].

5 数值仿真

本节主要对前文所提到的密钥生成方案进行数值仿真, 测试该方案在瑞利衰落信道条件下的性能. 分别在准静态及慢衰落信道场景下, 对比传统从随机变化的信道参数中提取密钥的方案与本文所提方案, 仿真研究: ①本文提出方法的密钥速率与信噪比之间的关系; ②本文提出方法的密钥速率在固定信噪比条件下与发送端天线数之间的关系.

假设传统方法采用每根天线分别发送导频的方法估计信道, 导频序列包含 128 个符号, 因此每次从发端发送导频到收端估计出信道并提取密钥所消耗时间为 $T_P = 128T$. 同样假设本文所提方法中, 每次从发端发送随机信号到收端接收信号并提取密钥所消耗时间为 T. 如图 2 所示, 假设在相干时间 T_C 内, Alice 共发送了 M 次随机信号矢量, 则整个密钥生成过程消耗时间为 $T_1 = N_B T_P + (K+M)T$. 对于传统方法来说, 通信双方每根天线均需要发送导频并估计信道, 因此整个密钥生成过程消耗时间为 $T_2 = (N_A + N_B)T_P$.

文献 [14] 中提出了一种利用 Copula 熵估计一维随机变量间互信息的方法. 为满足仿真需要, 此处利用互信息及香农熵的定义式将该互信息估计方法推广到估计多维随机变量的条件互信息, 即

$$\begin{aligned} & I(X_1,\ldots,X_l;Y_1,\ldots,Y_m|Z_1,\ldots,Z_n) \\ & \quad = I(X_1,\ldots,X_l;Y_1,\ldots,Y_m;Z_1,\ldots,Z_n) \\ & \qquad - I(X_1,\ldots,X_l;Z_1,\ldots,Z_n) \\ & \qquad - I(Y_1,\ldots,Y_m;Z_1,\ldots,Z_n) + I(Z_1,\ldots,Z_n), \qquad (21) \end{aligned}$$

仿真中采用该方法, 对 Alice 计算所得的 Bob 的接收信号矢量与 Bob 实际接收信号矢量, 在 Eve 被动窃听条件下的互信息, 即密钥速率进行估计. 仿真结果为在随机生成 10^4 次信道条件下, 求得的平均密钥速率, 单位为 bit/T.

5.1 准静态信道场景

在准静态信道条件下, 信道参数依然为随机变量, 但在多次密钥生成过程中几乎保持不变. 因此对于传统方法来说, 密钥速率将严重受限. 而本文所提方法还利用了发送信号的随机性来提高密钥速率, 在该场景下仍可以取得较好的结果. 此时 $T_C \to \infty$, 因此 $M \gg N_B T_P/T + K$, $T_1 \approx MT$.

仿真中, 主信道 $\boldsymbol{H}_B$ 与窃听信道 $\boldsymbol{H}_E$ 相互独立, 且均服从均值为 0, 方差为 1 的复高斯分布. 噪声功率为 0dBm.

图 3 中分析了该场景下密钥生成方案在不同信噪比条件下的平均密钥速率. 发送方 Alice 配备 8 根天线, 接收方 Bob 配备 2 根天线, 窃听方 Eve 配备 10 根天线. 其中密钥速率极限由文献 [9] 给出, 如下式所示:

$$\lim_{P\to\infty} C_s(P) = \sum_i \log\left(1+\tilde{\sigma}_i^2\right), \tag{22}$$

式 (22) 中 $\tilde{\sigma}_i$ 为 $\left(\hat{\boldsymbol{H}}_B, \hat{\boldsymbol{H}}_E\right)$ 的广义奇异值. 如图 3 所示, 平均密钥速率随着信噪比地提高而上升. 在信道为准静态条件下, 信道参数变化极慢. 在该条件下, 采用传统从信道参数中提取密钥的方法, 单位时间内得到的密钥长度很小. 本文所提方法的密钥速率由信道的随机性及发送信号的随机性两方面决定, 即使信道参数不变也能够生成密钥. 所提方法从接收信号中提取密钥, 因此在高信噪比条件下窃听方也会获得更多与密钥相关的信息, 故密钥速率受限. 当能够得知窃听信道的 CSI 时, 既可以针对当前的信道条件合理分配功率, 即采用 4.2 节的性能优化方法来提高密钥速率. 在低信噪比条件下, 性能优化效果比较明显. 随着信噪比地提高, 信道参数对于接收信号结果的影响越来越小, 发送信号经历不同信道后出现的差异同样逐渐变小, 因此优化效果受限.

图 4 中分析了接收端天线数变化条件下的密钥速率. 接收方 Bob 配备 2 根天线, 窃听方 Eve 配备 10 根天线. 发送方 Alice 配备天线数从 2 到 8 变化. 发方天线数增多时, 发送的随机信号矢量维数增多, 尽管接收信号空间的维数没变, 但对于窃听方来说, 增加的随机信号影响了窃听方的接收效果, 因此密钥速率上升. 同时也可以看出, 当 Alice 与 Bob 天线数量的差距较大时, 本文所提方案在性能上更具优势.

5.2 慢衰落信道场景

在慢衰落信道场景下, 传统方法与本文所提方法均可以利用信道本身的随机性生成密钥. 因此在该场景下, 传统方法与本文所提方法均能够有效地生成密钥. 假设此时相干时间 $T_C = T_2 = (N_A + N_B)T_P$, 即采用传统方法时, 通信双方能够在相干时间内完成信道估计.

图 5 为该场景中密钥生成方案在不同信噪比条件下的平均密钥速率. 发送方 Alice 配备 8 根天线, 接收方 Bob 配备 2 根天线, 窃听方 Eve 配备 10 根天线. 随着信噪比地提高, 噪声所造成的影响减小, 信道估计的结果更加准确, 因此 Alice 与 Bob 生成密钥的一致性提高, 密钥速率呈上升趋势. 图 6 为该场景中密钥生成方案在不同发送天线数条件下的平均密钥速率. 接收方 Bob 配备 2 根天线, 窃听方 Eve 配备 10 根天线, 发送方 Alice 配备天线数从 2 到 8 变化. 与图 4 结果类似, 密钥速率随 Alice 天线数地增加而提高. 传统方法采用从无线信道参数中提取密钥的方法, 因此需要发送导频序列进行信道估计. 当天线数较多时, 相对于信号接收过程来说, 信道估计过程将消耗大量时间. 所以在单位时间

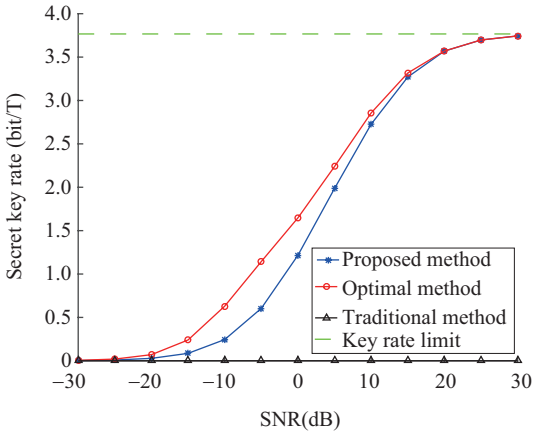


图 3 (网络版彩图) 平均密钥速率随 SNR 的变化曲线 (准静态)

Figure 3 (Color online) Average secret key rate as a function of SNR(quasi-static channel)

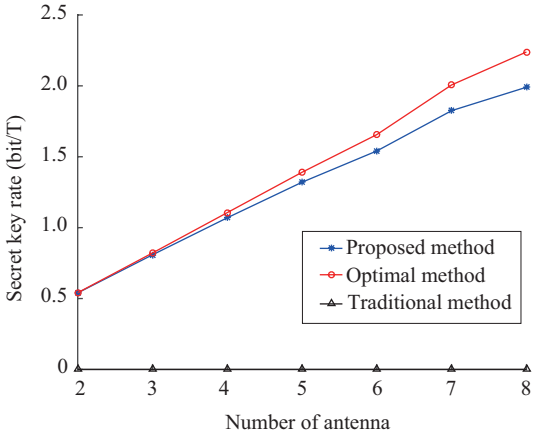


图 4 (网络版彩图) 平均密钥速率随天线数的变化曲线 (准静态)

Figure 4 (Color online) Average secret key rate as a function of antenna number(quasi-static channel)

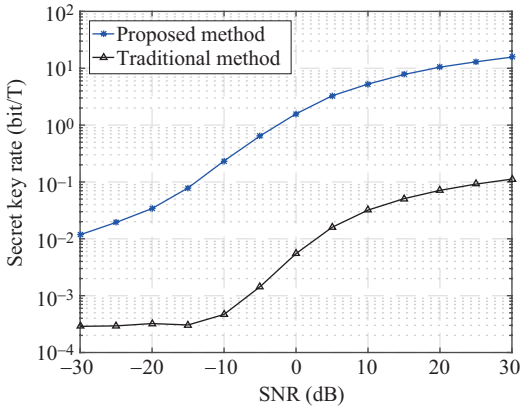


图 5 (网络版彩图) 平均密钥速率随 SNR 的变化曲线 (慢衰落)

Figure 5 (Color online) Average secret key rate as a function of SNR(slow-fading channel)

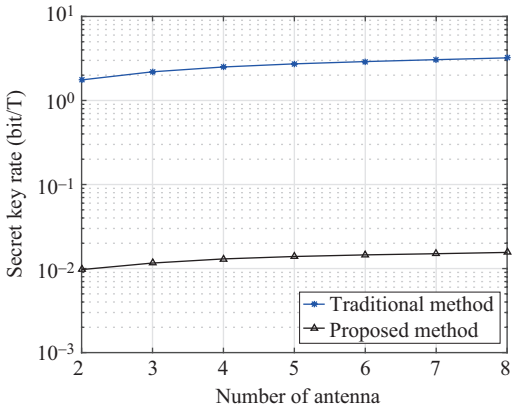


图 6 (网络版彩图) 平均密钥速率随天线数的变化曲线 (慢衰落)

Figure 6 (Color online) Average secret key rate as a function of antenna number(slow-fading channel)

内, 采用传统方法得到的密钥速率较低. 本文所提的密钥生成方法则只要求发送方 Alice 估计信道, 而接收方 Bob 只需要对接收的信号进行采样量化处理, 减小了开销, 故能取得较高的密钥速率. 另外相干时间更长, 即 $T_C > T_2$ 时, 由于信道参数不变, 采用传统方法将无法继续生成新的密钥, 而本文方法则能够通过 Alice 发送随机信号改变 Bob 的接收信号, 继续生成新的密钥.

6 结束语

本文主要讨论了基于接收信号空间的密钥生成方法. 首先给出了密钥提取模型, 并在此基础上得

到基于 MIMO 接收信号空间的密钥生成原理, 即 MIMO 信道确定接收信号空间, 合法通信双方可在空间中随机选取相同元素生成密钥, 从而克服信道慢变带来的密钥速率低下问题. 之后为解决合法通信双方分别从同一接收信号空间中提取相同密钥的问题, 给出具体的密钥提取方法, 分析了该密钥生成方案的安全性能. 最后给出在准静态及慢衰落信道条件下的仿真结果, 说明该方案的有效性.

参考文献

1 Jakes W C, Cox D C. Microwave Mobile Communications. Piscataway: Wiley-IEEE Press, 1994, 11–50

2 Maurer U M. Secret keyagreement by public discussion from common information. IEEE Trans Inf Theory, 1993, 39: 733–742

3 Ahlswede R, Csiszar I, Ahlswede R. Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans Inf Theory, 1993, 39: 1121–1132

4 Hershey J E, Hassan A A, Yarlagadda R. Unconventional cryptographic keying variable management. IEEE Trans Commun, 1995, 43: 3–6

5 Aono T, Taromaru K, Ohira T, et al. Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: RSSI interleaving scheme. In: Proceedings of European Conference on Wireless Technology, Paris, 2006. 173–176

6 Lai L, Liang Y, Du W. Cooperative key generation in wireless networks. IEEE J Sel Areas Commun, 2012, 30: 1578–1588

7 Premnath S N, Jana S, Croft J. Secret key extraction from wireless signal strength in real environments. IEEE Trans Mobile Comput, 2013, 12: 917–930

8 Yang B, Wang W, Yin Q. Secret key generation from multiple cooperative helpers by rate unlimited public communication. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing. New York: IEEE Press, 2014. 8183–8187

9 Renna F, Bloch M R, Laurenti N. Semi-blind key-agreement over MIMO fading channels. IEEE Trans Commun, 2013, 61: 620–627

10 Khisti A, Wornell G W. Secure transmission with multiple antennas–part II: the MIMOME wiretap channel. IEEE Trans Inf Theory, 2010, 56: 5515–5532

11 Zeng K, Wu D, Chan A, et al. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: Proceedings of the IEEE International Conference on Computer Communications. New York: IEEE Press, 2010. 1–9

12 Cumanan K, Ding Z, Sharif B, et al. Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper. IEEE Trans Veh Tech, 2014, 63: 1678–1690

13 Beck A, Ben-Tal A, Tetruashvili L. A sequential parametric convex approximation method with applications to nonconvex truss topology design problems. J Global Optim, 2009, 47: 29–51

14 Zeng X, Durrani T. Estimation of mutual information using copula density function. Electron Lett, 2011, 47: 493–494

附录 A 式 (16) 密钥速率计算

在本文的密钥生成模型中, Bob 与 Eve 的接收信号在已知 Alice 发送信号的条件下相互独立, 且 $\boldsymbol{r}=\boldsymbol{s}+\hat{\boldsymbol{w}}_B$. 由文献 [3] 可知, 密钥速率可以由下式表示:

$$C_s = I\left(\boldsymbol{s};\boldsymbol{r}|\boldsymbol{z}\right) = h\left(\boldsymbol{r}|\boldsymbol{z}\right) - h\left(\boldsymbol{r}|\boldsymbol{s},\boldsymbol{z}\right) = h\left(\boldsymbol{r},\boldsymbol{z}\right) - h\left(\boldsymbol{z}\right) - h\left(\hat{\boldsymbol{w}}_B\right), \tag{A1}$$

所以, 在此密钥生成模型中, 密钥速率 C_s 与 Alice 用于密钥生成的信号 $\boldsymbol{s}$ 无关. 与文献 [9] 中问题类似, 推导 MIMO 系统密钥速率如下:

$$\begin{aligned} C_s &= \log\left(\pi e\right)^{N_B+N_E}\left|\mathrm{E}\begin{bmatrix}\boldsymbol{r}\boldsymbol{r}^{\mathrm{H}} & \boldsymbol{r}\boldsymbol{z}^{\mathrm{H}}\\ \boldsymbol{z}\boldsymbol{r}^{\mathrm{H}} & \boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\end{bmatrix}\right| - \log\left(\pi e\right)^{N_E}\left|\mathrm{E}\left[\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\right]\right| - \log\left(\pi e\right)^{N_B}\\ &= \log\left|\mathrm{E}\left[\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\right]\right|\left|\mathrm{E}\left[\boldsymbol{r}\boldsymbol{r}^{\mathrm{H}}\right] - \mathrm{E}\left[\boldsymbol{r}\boldsymbol{z}^{\mathrm{H}}\right]\left(\mathrm{E}\left[\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\right]\right)^{-1}\mathrm{E}\left[\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\right]\right| - \log\left|\mathrm{E}\left[\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\right]\right| \end{aligned}$$

$$= \log\left|\boldsymbol{I}+\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\left(\hat{\boldsymbol{H}}_B^{\mathrm{H}}\hat{\boldsymbol{H}}_B+\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\right| - \log\left|\boldsymbol{I}+\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\boldsymbol{K}_{\boldsymbol{xx}}^{\frac{1}{2}}\right| > 0, \tag{A2}$$

可得式 (16) 结果.

附录 B 式 (19) 泰勒级数展开

令 $g(\boldsymbol{p}) = \log\left|\boldsymbol{K}_{\boldsymbol{xx}}+\left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right|$, 对 $g(\boldsymbol{p})$ 在 $\tilde{\boldsymbol{p}}$ 处进行一阶泰勒级数展开, 则在 $\tilde{\boldsymbol{p}}$ 附近存在

$$g(\boldsymbol{p}) \approx g(\tilde{\boldsymbol{p}}) + g'(\tilde{\boldsymbol{p}})^{\mathrm{T}}(\boldsymbol{p}-\tilde{\boldsymbol{p}}), \tag{B1}$$

其中 $g'(\tilde{\boldsymbol{p}})$ 为 $g(\boldsymbol{p})$ 的一阶偏导数向量在 $\tilde{\boldsymbol{p}}$ 处的取值, 由于

$$\frac{\partial g}{\partial p_i} = \frac{1}{\ln 2}\left[\left(\boldsymbol{K}_{\boldsymbol{xx}}+\left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right)^{-1}\right]_{ii}, \tag{B2}$$

所以

$$g'(\boldsymbol{p}) = \frac{\partial g}{\partial \boldsymbol{p}} = \frac{1}{\ln 2}\mathrm{diag}\left(\left(\boldsymbol{K}_{\boldsymbol{xx}}+\left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right)^{-1}\right), \tag{B3}$$

其中 $[\cdot]_{ij}$ 表示位于矩阵第 i 行 j 列的元素. 将式 (B3) 代入式 (B1) 可得:

$$g(\boldsymbol{p}) \approx \log\left|\tilde{\boldsymbol{K}}_{\boldsymbol{xx}}+\left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right| + \frac{1}{\ln 2}\left[\mathrm{diag}\left(\left(\tilde{\boldsymbol{K}}_{\boldsymbol{xx}}+\left(\hat{\boldsymbol{H}}_E^{\mathrm{H}}\hat{\boldsymbol{H}}_E\right)^{-1}\right)^{-1}\right)\right]^{\mathrm{T}}(\boldsymbol{p}-\tilde{\boldsymbol{p}}), \tag{B4}$$

最后将式 (B4) 代入式 (18) 可得式 (19).

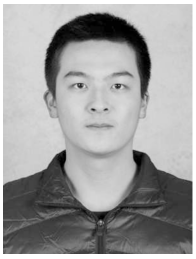
Secret key generation scheme based on MIMO received signal spaces

Yangming LOU, Liang JIN*, Zhou ZHONG, Kaizhi HUANG & Shengjun ZHANG

China National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002*, China*
*Corresponding author. E-mail: liangjin@263.net

Abstract Conventional secret key generation scheme cannot achieve high key generation rate when the channel characteristics change slowly. To solve this problem, a secret key generation model based on the MIMO received signal space is investigated in this paper. In this model, the legitimate transmitter and receiver distill secret keys from the received signal space, and improve the randomness of the received signals by controlling the variance of the transmitted signals, so that the update of the secret key is independent of the time variance of the wireless channel. Then a specific key generation scheme is proposed, in which the legitimate nodes can obtain the same received signal space, from which common vectors can be selected to distill the keys. In addition, an optimal power allocation method to maximize the key rate is presented. The results of the simulation confirm the effectiveness of this scheme.

Keywords physical layer security, secret key generation, MIMO system, received signal space, power allocation



Yangming LOU was born in 1991. He received his Master's degree from the National Digital Switching System Engineer & Technological Research Center, Zhengzhou, in 2016. His research interests include wireless communication security and secret key generation.

Liang JIN was born in 1969. He received his Ph.D. degree from Xi'an Jiaotong University, Xi'an, in 1999. Currently, he is a professor at the National Digital Switching System Engineering & Technological Research Center(NDSC). His research interests include ultra wideband wireless communication and smart antenna.