中国科学: 信息科学 2014 年 第 44 卷 第 11 期: 1482–1494
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

论 文

基于多节点分组协作干扰的无线物理层安全传输

邓浩[①②], 王慧明[①*], 王文杰[①]

① 西安交通大学电子与信息工程学院, 智能网络与网络安全教育部重点实验室, 西安 710049
② 河南大学物理与电子学院, 开封 475004
* 通信作者. E-mail: hmwang@mail.xjtu.edu.cn

收稿日期: 2014–03–06; 接受日期: 2014–07–08
国家自然科学基金 (批准号: 61102081, 61172092)、国家自然科学基金创新群体 (批准号: 61221063)、教育部新世纪优秀人才支持计划 (批准号: NCET-13-0458)、霍英东青年教师基金 (批准号: 141063) 和中央高校基本科研业务费 (批准号: 2013jdgz11) 资助项目

摘要 针对无线通信的安全传输问题, 提出了一种新的多节点分组协作干扰以增强安全的策略. 在源节点发送私密信息的同时, 传统协作干扰策略中所有的协作节点发送公共的人工噪声干扰窃听用户, 而分组协作干扰策略中协作节点分组发送不同的人工噪声. 为了保证人工噪声不干扰目的节点, 协作干扰策略的波束形成系数的设计基于迫零准则. 在节点独立功率约束的条件下, 传统干扰策略无法有效的利用所有协作节点的阻塞功率, 而分组干扰策略将每两个信道增益接近的节点划分为一组, 从而保证组内的协作节点能近乎完全利用可用的阻塞总功率. 仿真结果验证了最小距离分组干扰策略利用的阻塞总功率最大, 也对应最大的平均安全速率. 为更易于实现, 文中还提出了基于相对距离的固定分组策略. 除此之外, 文中还考虑了人工噪声泄露的情况, 此时传统协作干扰策略完全失效, 而分组协作干扰策略即便是只有一组有效, 也可以保证平均安全速率依然随协作节点最大发射功率增大而增大. 实验结果证实了分组协作干扰策略要优于传统协作干扰策略.

关键词 物理层安全 协作干扰 多节点协作 人工噪声 分组协作

1 引言

无线通信由于其易于接入的便利性, 已经得到了广泛使用. 但由于无线信道固有的广播特性, 使得无线通信更易于被非法用户窃听. 保密通信的目的在于保证合法用户之间可靠安全的通信, 而窃听用户在通信过程中无法获取合法用户的信息. 传统的无线安全都是在高层进行数据加密 [1], 而物理层安全能充分利用无线信道的特征以增强安全, 近年来吸引了大量研究者的关注 [2~6]. Wyner[7] 最早提出了安全容量的定义, 用以度量合法用户之间可靠安全通信的最大信息传输速率. 在衰落信道中, 只有在合法用户的信道状态优于窃听用户信道的情况下, 安全容量才不为零. 利用节点协作技术可以保证即便在合法用户的信道状态差于窃听用户的情况下, 依然可以获得正的安全速率. 多节点协作增强安全的方法主要有两种: 协作波束形成 [2,3] 与协作干扰 [2~4]. 在协作波束形成策略中, 协作节点以放大转发 (amplify-and-forward, AF) 或者译码转发 (decode-and-forward, DF) 的方式向目的节点转发源节点的私密信息. 通过协作波束形成, 可以有效地提高目的节点的接收信噪比 (signal to noise ratio, SNR).

引用格式: 邓浩, 王慧明, 王文杰. 基于多节点分组协作干扰的无线物理层安全传输. 中国科学: 信息科学, 2014, 44: 1482–1494, doi: 10.1360/N112014-00048

https://engine.scichina.com/doi/10.1360/N112014-00048

在协作干扰策略中, 多节点通过协作发送人工噪声/阻塞信号 (artificial noise/jamming signal), 使其对窃听节点的损害大于对目的节点的影响, 从而达到提升系统安全性能的目的 (如提高安全速率或降低安全中断率). 在这两种不同的策略中, 协作节点扮演了不同的角色, 一种是中继转发节点, 另一种是阻塞节点. 在大多文献中, 协作节点都扮演着单一角色. 在最近的文献 [5] 中, 作者提出了一种混合协作波束形成与协作干扰的传输策略, 该策略选择其中一部分节点作为中继转发信息, 而另外一部分节点发送人工噪声干扰窃听用户. 在文献 [6] 中, 作者提出了另外一种协作策略, 噪声转发 (noise-foewarding, NF), 协作节点发送独立于信息码字的公开码字. 若协作节点距离合法节点很近, 则合法用户有高的概率对接收到的干扰码字正确译码, 继而从接收信号中消除干扰码字. 而窃听用户接收到干扰码字的信噪比很低, 无法正确译码, 相当于增大了窃听用户的噪声功率, 从而降低了窃听用户的信噪比.

需要指出的是, 由于体积及功耗方面的考虑, 协作通信中的节点大多配置的是单天线, 使得节点通信只能工作在单工模式下. 当节点采用协作波束形成策略时, 由于单工模式的限制, 每个私密信息需要两个时隙才能完成从源节点到目的节点的传输. 两个时隙传输不可避免地降低了系统频谱效率, 而且信息泄露在每个时隙都会发生, 也增加了窃听用户获取私密信息的可能性. 若采用协作干扰策略, 私密信息的传输只需要一个时隙. 基于上述原因, 本文考虑采用协作干扰的方式以增强安全. 在每一个时隙, 当目的节点发送私密信息的时候, 所有的协作节点同时发送干扰信号. 一种显然的策略是干扰信号位于合法用户信道矩阵的零空间 (该策略称之为迫零策略), 从而保证合法用户不受到人工噪声的干扰. 文献 [8] 证实在高功率情况下, 迫零策略是渐进最优的. 在文献 [9] 中, 作者考虑了两种干扰策略: 协作节点发送公共的人工噪声与协作节点发送独立的人工噪声, 并从目的节点与窃听节点接收信噪比概率分布的角度分析了这两种传输策略的能量效率. 合理的设计协作节点发送公共人工噪声的波束形成系数, 可以使得合法用户不受到干扰, 但是需要协作节点在通信前共享生成人工噪声的公共信息, 从而导致窃听用户可能获得人工噪声的信息, 使得协作干扰的性能降低, 甚至失效. 而协作节点发送独立的人工噪声无法保证合法用户不受到干扰, 也不能保证合法用户受到的干扰轻于窃听用户. 从这个角度出发, 本文考虑将协作节点分组, 每组包含两个节点, 每组之间发送独立的人工噪声并在合法用户处形成零陷. 分组干扰策略既可以保证不干扰目的节点, 也能保证生成人工噪声的信息只需要在局部的组内之间共享. 即便是某一组的干扰信号泄露, 系统性能也不会明显下降.

当多节点之间协作的时候, 功率分配是影响性能的一个重要因素. 在文献 [10 ∼ 12] 中, 作者考虑了总功率约束情况下的功率分配. 而更实际的情况是通信中的节点都受到独立功率约束. 在文献 [4,13], 作者考虑了独立功率约束下的波束形成系数设计, 但功率分配的设计依赖于瞬时信道信息, 甚至依赖于窃听用户的瞬时信道信息. 而更一般的情况是系统仅知道窃听用户的统计信道信息, 或者对窃听用户的位置信息也一无所知. 在没有窃听用户信道信息的情况下, 文献 [4,13] 中协作干扰策略的性能会严重下降. 而本文所考虑的干扰策略不依赖于窃听用户信道的实时信息, 因此具有更实际的意义. 另外需要注意的是在迫零准则下考虑协作干扰的波束形成, 即便是最佳的波束形成系数也无法充分利用所有节点的阻塞功率. 原因在于协作节点与目的节点之间的信道独立且不同分布, 其实时信道增益之间可能差别很大, 因此各个节点在满足独立功率约束的前提下无法充分利用自身功率. 若把每两个节点划分成一组进行协作, 合理的分组能保证每组内节点的信道增益近似相等, 至少差别不大, 从而保证协作节点能更充分地利用阻塞功率. 到目前为止, 分组协作以增强无线通信安全的研究文献还相对比较少. 在文献 [14,15] 中作者将协作节点分为干扰组和中继组, 干扰组既发送人工噪声也发送私密信号. 文献 [14] 中作者没有考虑如何对协作节点分组, 只是简单地比较了分组中节点个数对性能的影响, 而文献 [15] 只是选择其中一个协作节点作为阻塞节点.

本文中, 用小写字母表示标量, 用粗体小写和粗体大写字母表示向量和矩阵, $\mathrm{E}[x]$ 分别表示 x 的

https://engine.scichina.com/doi/10.1360/N112014-00048

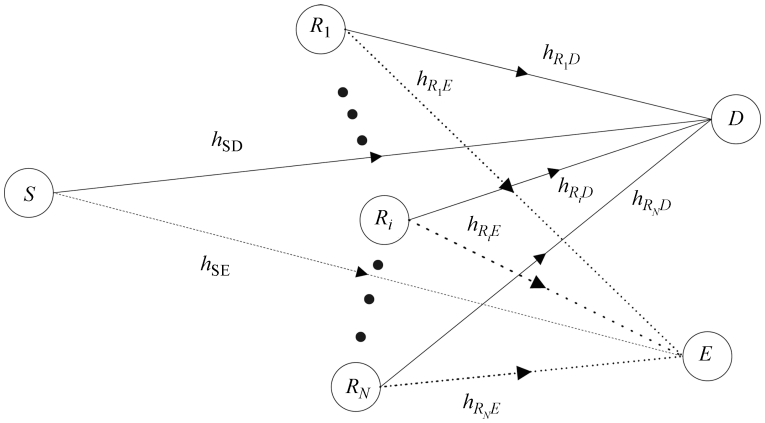


图 1　系统模型

Figure 1　System model

期望, $|x|$ 表示 x 的模值. $\boldsymbol{x}^{\mathrm{T}}, \boldsymbol{x}^{\mathrm{H}}, \boldsymbol{x}^{*}$ 分别表示向量 $\boldsymbol{x}$ 的转置、共轭转置及共轭. $\mathrm{tr}\,(\boldsymbol{X})$ 表示矩阵 $\boldsymbol{X}$ 的迹, $\mathrm{rank}\,(\boldsymbol{X})$ 表示矩阵 $\boldsymbol{X}$ 的秩, $(x)^{+} = \max(x, 0)$, $\mathrm{diag}\,(\boldsymbol{x})$ 表示将向量 $\boldsymbol{x}$ 中的元素构建为一个对角矩阵.

2　系统模型及问题描述

2.1　系统模型

协作通信网络的系统模型如图 1 所示. 网络中包含一个源节点 S、一个目的节点 D、一个窃听节点 E 和 N 个协作节点 R_i, 其中 $i \in (1, \ldots, N)$. 网络中所有的节点均为单天线节点. 假设信道增益满足 $h_{\mathrm{mn}} = d_{\mathrm{mn}}^{-\frac{c}{2}} g_{\mathrm{mn}}$, 其中 $m \in S, R_i$, $n \in D, E, R_i$, g_{mn} 服从零均值单位方差的复高斯分布, d_{mn} 表示节点 m 与节点 n 之间的距离, c 表示路径损耗指数 (一般在 2 和 6 之间). 不失一般性, 假设网络中所有节点处的加性噪声都是零均值复高斯白噪声, 且具有相同的方差 δ^2. 假设 E 与 D 之间存在直达径, 则源节点可以直接传输私密信号 s 到目的节点, 其发送信号的平均功率为 P_s, 且私密信号 s 服从高斯分布. 在源节点发送私密信号的同时, 全体协作节点发送人工噪声干扰窃听节点, 假设协作节点发送人工噪声的最大功率为 P_z.

2.2　基于协作干扰的安全传输

在协作干扰策略中, 当源节点发送私密信号 s 时, N 个协作节点同时发送公共的人工噪声 z. 为了描述的方便, 将这种协作节点发送公共人工噪声的策略称为传统协作干扰策略. 为达到安全容量, 假设 s 和 z 服从标准高斯分布. 波束形成系数 $\boldsymbol{w}$ 由 $\boldsymbol{h}_{\mathrm{RD}}$ 的零空间张成, 其中 $\boldsymbol{w} = [w_1^*, \ldots, w_N^*]^{\mathrm{T}}$, $\boldsymbol{h}_{\mathrm{RD}} = [h_{\mathrm{R_1D}}, \ldots, h_{\mathrm{R}_N\mathrm{D}}]^{\mathrm{T}}$, 则 $\boldsymbol{w}$ 满足 $\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{RD}} = 0$. 目的节点与窃听节点接收到的信号分别为

$$r_D = \sqrt{P_s} h_{\mathrm{SD}} s + n_D, \tag{1}$$

$$r_E = \sqrt{P_s} h_{\mathrm{SE}} s + \boldsymbol{w}^{\mathrm{H}} \boldsymbol{h}_{\mathrm{RE}} z + n_E, \tag{2}$$

其中, P_s 表示信号功率, $\boldsymbol{h}_{\mathrm{RE}} = [h_{\mathrm{R_1E}}, \ldots, h_{\mathrm{R}_N\mathrm{E}}]^{\mathrm{T}}$.

https://engine.scichina.com/doi/10.1360/N112014-00048

由式 (1) 和 (2) 可以得到目的节点与窃听节点的信噪比分别为

$$\Gamma_D = \frac{P_s|h_{\mathrm{SD}}|^2}{\delta^2}, \tag{3}$$

$$\Gamma_E = \frac{P_s|h_{\mathrm{SE}}|^2}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{RE}}\boldsymbol{w}+\delta^2}, \tag{4}$$

其中 $\boldsymbol{H}_{\mathrm{RE}} = \boldsymbol{h}_{\mathrm{RE}}\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}$. 瞬时安全速率可以表示为

$$\begin{aligned} R_s =& \left(\log_2(1+\Gamma_D) - \log_2(1+\Gamma_E)\right)^+ \\ =& \left(\log_2\left(1+\frac{P_s|h_{\mathrm{SD}}|^2}{\delta^2}\right) - \log_2\left(1+\frac{P_s|h_{\mathrm{SE}}|^2}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{RE}}\boldsymbol{w}+\delta^2}\right)\right)^+. \end{aligned} \tag{5}$$

从式 (5) 可知最大化安全速率等同于最大化窃听节点 E 接收的人工噪声功率, 则协作干扰的波束形成系数优化设计问题可以描述如下:

$$\begin{cases} \max\limits_{\boldsymbol{w}} \ \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{RE}}\boldsymbol{w}, \\ \text{s.t.} \quad \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{RD}} = 0, \quad |w_i|^2 \leqslant P_z, i = 1, \ldots, N. \end{cases} \tag{6}$$

在实际情况中, 窃听节点在网络中都是被动的接收信号, 合法用户无法获取窃听用户的信道信息, 甚至无法确定是否有窃听用户存在. 在无法获取窃听用户瞬时信道信息的情况下, $\boldsymbol{H}_{\mathrm{RE}}$ 未知, 此时无法通过搜索最优的 $\boldsymbol{w}$ 以获得最大的瞬时安全速率. 由于每个协作节点都受到功率约束, 很显然用于人工噪声的总功率越大, 对窃听用户的干扰会更严重. 为此式 (6) 中的优化目标可以修改为最大化人工噪声的总功率 $\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}$, 则优化问题可以描述为如下:

$$\begin{cases} \max\limits_{\boldsymbol{w}} \ \boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}, \\ \text{s.t.} \quad \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{RD}} = 0, \quad |w_i|^2 \leqslant P_z, i = 1, \ldots, N. \end{cases} \tag{7}$$

将 $\boldsymbol{h}_{\mathrm{RD}}$ 的零空间表示为 $\boldsymbol{h}_{\mathrm{RD}}^{\perp}$, 则波束形成系数可以表示为 $\boldsymbol{w} = \boldsymbol{h}_{\mathrm{RD}}^{\perp}v$, 其中 v 为服从高斯分布的 $N\times 1$ 维随机矢量. 式 (7) 中的优化问题等价为

$$\begin{cases} \max\limits_{\boldsymbol{v}} \ \boldsymbol{v}^{\mathrm{H}}\boldsymbol{R}\boldsymbol{v}, \\ \text{s.t.} \quad \boldsymbol{v}^{\mathrm{H}}\boldsymbol{A}_i\boldsymbol{v} \leqslant P_z, i = 1, \ldots, N, \end{cases} \tag{8}$$

其中 $\boldsymbol{R} = \boldsymbol{h}_{\mathrm{RD}}^{\perp\ \mathrm{H}}\boldsymbol{h}_{\mathrm{RD}}^{\perp}$, $\boldsymbol{A}_i = \boldsymbol{h}_{\mathrm{RD}}^{\perp}(i,:)^{\mathrm{H}}\boldsymbol{h}_{\mathrm{RD}}^{\perp}(i,:)$, $\boldsymbol{h}_{\mathrm{RD}}^{\perp}(i,:)$ 表示 $\boldsymbol{h}_{\mathrm{RD}}^{\perp}$ 的第 i 行行向量. 令 $\boldsymbol{V} = \boldsymbol{v}\boldsymbol{v}^{\mathrm{H}}$, 注意到 $\boldsymbol{v}^{\mathrm{H}}\boldsymbol{R}\boldsymbol{v} = \mathrm{tr}(\boldsymbol{R}\boldsymbol{V})$, $\boldsymbol{v}^{\mathrm{H}}\boldsymbol{A}_i\boldsymbol{v} = \mathrm{tr}(\boldsymbol{A}_i\boldsymbol{V})$, 式 (8) 中的优化问题可以等价为

$$\begin{cases} \max\limits_{\boldsymbol{V}} \ \mathrm{tr}(\boldsymbol{R}\boldsymbol{V}), \\ \text{s.t.} \quad \mathrm{tr}(\boldsymbol{A}_i\boldsymbol{V}) \leqslant P_z, i = 1, \ldots, N, \quad \boldsymbol{V} \succeq 0, \mathrm{rank}(\boldsymbol{V}) = 1. \end{cases} \tag{9}$$

上述优化问题为二次约束二次规划 (quadratically constrained quadratic program, QCQP), 一般情况下其为非凸问题, 求解 QCQP 问题为 (non-deterministic polynomial, NP) 难问题. 若将 QCQP 问题松弛为半正定规划 (semidefinite program, SDP), 式 (9) 在多项式时间内可以得到近似解. 式 (9) 中的 QCQP 问题可以松弛为下述 SDP 问题

$$\begin{cases} \max\limits_{\boldsymbol{V}} \ \mathrm{tr}(\boldsymbol{R}\boldsymbol{V}), \\ \text{s.t.} \quad \mathrm{tr}(\boldsymbol{A}_i\boldsymbol{V}) \leqslant P_z, i = 1, \ldots, N, \quad \boldsymbol{V} \succeq 0. \end{cases} \tag{10}$$

https://engine.scichina.com/doi/10.1360/N112014-00048

注意式 (10) 中的 SDP 问题与式 (9) 中的 QCQP 问题的区别在于 SDP 问题中去掉了约束条件 $\mathrm{rank(V)}=1$, 由于 SDP 为凸问题, 可以方便地利用内点法进行求解. 但是也需要注意到 SDP 求解出的 $\boldsymbol{V}$ 一般情况下秩不为 1, 无法通过等式 $\boldsymbol{V}=\boldsymbol{v}\boldsymbol{v}^{\mathrm{H}}$ 求解出 $\boldsymbol{v}$. 在文献 [16] 中, 作者提出了一种高斯随机产生法以得到 $\boldsymbol{v}$ 的近似解. Algorithm 1 描述如下:

Algorithm 1 高斯随机产生法.

设 M 为整数.

(1) 产生 M 个 $(N-1)$ 维的随机矢量 $\boldsymbol{\xi}_m$, $m=1,\ldots,M$, 其服从复高斯分布 $\mathcal{CN}(0,\boldsymbol{V}^*)$. 令

$$\boldsymbol{v}(\boldsymbol{\xi}_m)=\boldsymbol{\xi}_m/\max_{1\leqslant i\leqslant N}\sqrt{\boldsymbol{\xi}_m^{\mathrm{H}}\boldsymbol{A}_i\boldsymbol{\xi}_m}.$$

(2) $\hat{\boldsymbol{v}}=\arg\ \max_{\boldsymbol{v}(\boldsymbol{\xi}_m),m=1,\ldots,N}\ |\boldsymbol{v}(\boldsymbol{\xi}_m)|^2$ 为式 (8) 的近似解.

利用高斯随机产生法得到的近似解 $\hat{\boldsymbol{v}}$, 代入方程 $\boldsymbol{w}=\boldsymbol{h}_{\mathrm{RD}}^{\perp}v$ 即可得到对应的最优解 $\hat{\boldsymbol{w}}$. 将 $\hat{\boldsymbol{w}}$ 代入到式 (5) 中即可得到系统的瞬时安全速率.

由于波束形成系数设计基于迫零准则, 则协作节点实际利用的阻塞总功率依赖于协作节点到目的节点之间的瞬时信道增益. 考虑一种极端情况, 在某个时刻, 即所有协作节点到目的节点的瞬时信道增益都相等, 此时模相同而相位不同的 $N\times 1$ 维矢量是 $\boldsymbol{w}$ 的解. 在这种情况下所有协作节点既充分利用了自身的阻塞功率, 也满足独立功率约束. 但在实际情况中, 这种情况出现的概率为零, 也就说明了尽管式 (6) 的近似解利用了相对最大的阻塞总功率, 但是不可能完全利用 NP_z 的可用阻塞总功率. 因此在独立功率约束的前提下, 如何保证充分利用每个节点的功率进行干扰是值得研究的问题.

另外需要指出的是, 在传统协作干扰策略中, 所有的协作节点发送公共的人工噪声. 这就要求在通信前, 系统中所有的节点都需要某种方式共享生成人工噪声的私密信息. 在文献 [11] 中, 作者提出协作双方通过安全传输种子以生成相同的人工噪声. 在文献 [17] 中, 作者假设所有合法用户通过伪随机码字的方式共享人工噪声的信息. 这两种共享方法的前提都是要求种子或者伪随机噪声只能合法用户已知, 但是显然在分享这些私密信息的时候有可能被窃听用户完全捕获, 从而窃听用户能完全消除人工噪声, 导致协作干扰策略完全失效.

除此之外, 利用内点法和高斯随机生成法求解协作干扰的最佳波束形成系数需要大量的计算量. 在节点功率有限的情况下, 若低复杂度的算法有更好的性能, 显然低复杂度的算法是更好的选择. 基于上述三个原因, 本文提出了如下分组协作干扰传输策略.

3 分组协作干扰的安全传输

在分组协作干扰策略中, 每两个协作节点按照一定的规则划分为一组. 假设系统中有 N 个不同的协作节点, 则组数为 $N/2$. 与传统协作干扰策略类似, 在通信前, 每组都需要提前共享生成人工噪声的私密信息. 但是与传统协作干扰策略不同的是, 分组干扰不同组发射的人工噪声是独立同分布的. 因此生成每组人工噪声的种子或者伪随机码字都是不同的. 在传统协作干扰策略中, 共享生成人工噪声的私密信息需要中心节点协调, 在这种情况下, 窃听用户可能会比某一些协作节点更靠近这个中心节点, 此时窃听用户接收到的信号可能会有更高的信噪比. 在保证所有协作节点都能可靠译码的情况下, 窃听用户也一定能可靠译码, 则可能导致人工噪声泄露. 在分组协作干扰策略中, 共享生成人工噪声的私密信息是在组间或者说是在局部进行的. 组间在分享私密信号的时候可以根据相对位置调整发射功率. 无论窃听用户处于任何位置, 都无法保证信噪比优于所有分组中的协作节点. 假设传统协作

https://engine.scichina.com/doi/10.1360/N112014-00048

干扰策略中, 窃听用户能完全译码人工噪声的概率为 P_E, 则分组协作干扰中人工噪声完全泄露的概率可以粗略近似为 $P_E^{N/2}$. 显然在 N 较大的时候, $P_E^{N/2}$ 要小得多, 也就是说分组协作干扰相比传统协作干扰要更鲁棒. 另外在分组协作策略中, 即便是某些组的人工噪声被窃听用户获取, 协作干扰的性能会下降, 但是不会严重到失效的程度.

分组协作干扰策略中每组协作的波束形成系数设计采用与传统协作干扰策略相同的迫零准则. 由于每组的协作节点为两个, 此时每组协作节点信道的零空间维数为 1, 波束形成系数即为零特征值对应的特征向量. 因此有无窃听用户的瞬时信道信息不影响分组策略的波束形成系数设计. 假设第 n 组中的协作节点为 R_{n1} 与 R_{n2}, 其发送的人工噪声为 z_n, 迫零向量为 $\boldsymbol{w}_n$, 其中 $R_{n1}, R_{n2} \in (R_i, i = 1, \ldots, N)$. 则分组策略下的瞬时安全速率可以表示成

$$R_s = \log_2\left(1 + \frac{P_s|h_{\mathrm{SD}}|^2}{\delta^2}\right) - \log_2\left(1 + \frac{P_s|h_{\mathrm{SE}}|^2}{\sum_{n=1}^{N/2} \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n + \delta^2}\right), \tag{11}$$

其中 $\boldsymbol{H}_{REn} = \boldsymbol{h}_{REn}{\boldsymbol{h}_{REn}}^{\mathrm{H}}$, $\boldsymbol{h}_{REn} = [h_{R_{n1}E}, h_{R_{n2}E}]^{\mathrm{T}}$. 很显然, 人工噪声策略的性能依赖于每组噪声在窃听节点处的接收功率, 每组的人工噪声发射功率越大, 则对窃听节点的干扰越大, 窃听节点的信噪比越低. 因此第 n 组协作节点的波束形成系数设计问题可以描述为如下的优化问题:

$$\begin{cases} \max\limits_{\boldsymbol{w}} & \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n, \\ \text{s.t.} & |w_{n,k}|^2 \leqslant P_z, k = 1, 2, \quad \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{h}_{RDn} = 0, \end{cases} \tag{12}$$

其中 $\boldsymbol{h}_{RDn} = [h_{R_{n1}D}, h_{R_{n2}D}]^{\mathrm{T}}$. 2×2 维矩阵 $\boldsymbol{h}_{RDn}{\boldsymbol{h}_{RDn}}^{\mathrm{H}}$ 的秩显然为 1, 设零特征值对应的向量为 $\boldsymbol{v}_n$, 则上述优化问题的解很容易表示为

$$w_{n,k} = \frac{\sqrt{P_z} v_{n,k}^*}{\max_{k=1,2} |v_{n,k}|}, k = 1, 2. \tag{13}$$

则第 n 组协作节点在窃听节点处的噪声功率贡献为

$$P_{j,n} = \frac{P_z \boldsymbol{v}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{v}_n}{\max_{k=1,2} |v_{n,k}|^2}. \tag{14}$$

综合上述分析, 可以得到全局的优化问题为

$$\max \quad \sum_{n=1}^{N/2} \frac{P_z \boldsymbol{v}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{v}_n}{\max_{k=1,2} |v_{n,k}|^2}. \tag{15}$$

3.1 分组策略

从式 (15) 可以看出, 不同的分组对应不同的信道状态和波束形成系数, 窃听节点处接收到的人工噪声总功率也不同. 因此存在一个最优的分组组合, 在最优分组组合下可以利用最大的阻塞总功率, 从而获得最大的安全速率. 由于信道之间是相互独立的, 获取最优的分组组合需要遍历所有的分组集合. 在 N 个协作节点的网络中, 一共有 C_N^2 种不同的分组. 在 N 很大的时候, 很难实现. 另外也需要注意到全局最优的分组组合依赖于窃听节点的瞬时信道信息. 本文只考虑未知窃听用户瞬时信道信息的情况, 因此只能给出局部最优的策略, 即使得每组协作节点发出的噪声总功率最大. 由于 $\boldsymbol{v}_n$ 是矩阵 $\boldsymbol{h}_{RDn}{\boldsymbol{h}_{RDn}}^{\mathrm{H}}$ 零特征值对应的特征向量, 其满足下列等式

$$v_{n,1}^* h_{R_{n1}D} + v_{n,2}^* h_{R_{n2}D} = 0. \tag{16}$$

https://engine.scichina.com/doi/10.1360/N112014-00048

由式 (16) 可以进一步推导出特征向量元素的模满足以下关系

$$\frac{|v_{n,1}|}{|v_{n,2}|}=\frac{|h_{R_{n2}D}|}{|h_{R_{n1}D}|}. \tag{17}$$

第 n 组发射人工噪声的总功率为

$$P_{t,n}=P_z\left(1+\frac{\min_{k=1,2}|v_{n,k}|^2}{\max_{k=1,2}\ \ |v_{n,k}|^2}\right). \tag{18}$$

在独立功率约束的条件下, 每组发射人工噪声总功率最大为 $2P_z$, 则满足 $\frac{\min_{k=1,2}|v_{n,k}|^2}{\max_{k=1,2}|v_{n,k}|^2}\leqslant 1$. 很显然 $\frac{\min_{k=1,2}|v_{n,k}|^2}{\max_{k=1,2}|v_{n,k}|^2}=1$ 的时候, 此时第 n 组协作节点完全利用了阻塞总功率 $2P_z$. 上述情况只有在 $|v_{n,1}|=|v_{n,2}|$ 的时候才成立. 由式 (18) 可知, 此时满足 $|h_{R_{n1}D}|=|h_{R_{n2}D}|$, 也就是说只有在第 n 组中的两个协作节点到目的节点的瞬时信道增益相等的时候才可能充分利用阻塞总功率. 在一般情况下不可能满足信道增益相等的条件, 但是这个结果暗示了当同组内的协作节点瞬时信道增益越接近, 发送的人工噪声总功率越大. 基于此, 本文给出了如下最小距离分组算法 (Algorithm 2).

Algorithm 2 最小距离分组法.

(1) 将 $|h_{R_iD}|$ 按照从小到大排列得到序列 $\boldsymbol{g}$, 计算前后元素的差值得到长度为 $N-1$ 的序列 $\boldsymbol{s}$.

(2) 找到 $\boldsymbol{s}$ 中最小的元素 $s(j)$, 则将序列 $\boldsymbol{g}$ 中第 j 个和第 $j+1$ 个元素作为第 1 组的元素.

(3) 删除元素 $g(j)$, $g(j+1)$. 顺序执行第 1,2 步, 直到 $N/2$ 个分组完成.

需要注意的是上述分组算法依赖于协作节点到目的节点的瞬时信道信息, 分组策略随信道状态的改变而改变. 因此需要在每个节点之间分享全局的合法节点之间的信道信息, 或者通过反馈信道由目的节点告知协作节点分组的结果. 更实际的算法是分组策略不依赖于实时信道, 一种自然的策略是将距离目的节点相对距离接近的协作节点划分为一组. 为此提出了下述基于相对距离的固定分组算法 (Algorithm 3).

Algorithm 3 固定分组法.

(1) 将 d_{R_iD} 按照从小到大排列得到序列 $\boldsymbol{d}$, 计算前后元素的差值得到长度为 $N-1$ 的序列 $\boldsymbol{r}$.

(2) 找到 $\boldsymbol{r}$ 中最小的元素 $r(j)$, 则将序列 $\boldsymbol{d}$ 中第 j 个和第 $j+1$ 个元素作为第 1 组的元素.

(3) 删除元素 $d(j)$, $d(j+1)$. 顺序执行第 1,2 步, 直到 $N/2$ 个分组完成.

3.2 性能分析

无论是传统协作干扰策略中, 还是在分组协作干扰策略中, 所有协作节点都是扮演阻塞节点的角色干扰窃听用户, 从而降低窃听用户的信噪比. 可以用概率 $P=\mathbb{P}\left(\Gamma_E\geqslant\gamma\right)$ 表征两种策略对窃听节点的损害程度 [9], 其中 γ 为给定的任意小的信噪比. 很显然 P 越小, 对窃听用户的损害越严重. 当 $P\to 0$ 时, 系统几乎没有中断发生, 此时也对应最大的平均安全速率. 对传统协作干扰策略而言, 可以计算其概率为

$$\begin{aligned}P_1&=\mathbb{P}\left(\frac{P_s|h_{\rm SE}|^2}{\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm RE}\boldsymbol{w}+\delta^2}\geqslant\gamma\right)\\&=\mathrm{E}_{\boldsymbol{h}_{REn}}\left[P_{h_{\rm SE}}\left(\frac{P_s|h_{\rm SE}|^2}{\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm RE}\boldsymbol{w}+\delta^2}\geqslant\gamma|\boldsymbol{h}_{\rm RE}\right)\right]\end{aligned}$$

https://engine.scichina.com/doi/10.1360/N112014-00048

$$= \mathrm{e}^{\frac{\gamma\delta^2 d_{\mathrm{SE}}^c}{P_s}} \mathrm{E}_{\boldsymbol{h}_{\mathrm{RE}}} \left[\mathrm{e}^{-\frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{RE}} \boldsymbol{w}} \right]. \tag{19}$$

利用文献 [18] 中的式 (14) 的结果, 式 (19) 中的期望可以计算如下:

$$\mathrm{E}_{\boldsymbol{h}_{\mathrm{RE}}} \left[\mathrm{e}^{-\frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{RE}} \boldsymbol{w}} \right] = \frac{1}{1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}^{\mathrm{H}} \mathrm{E}\left(\boldsymbol{H}_{\mathrm{RE}}\right) \boldsymbol{w}} = \frac{1}{1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \sum_{i=1}^{N} d_{R_i E}^{-c} |w_i|^2}. \tag{20}$$

综合式 (19) 和 (20) 中的结果, 可以得到概率 P_1 的最终表达式为

$$P_1 = \frac{\mathrm{e}^{\frac{\gamma\delta^2 d_{\mathrm{SE}}^c}{P_s}}}{1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \sum_{i=1}^{N} d_{R_i E}^{-c} |w_i|^2}. \tag{21}$$

对分组协作干扰策略而言, 可以计算其概率为

$$\begin{aligned} P_2 &= \mathbb{P}\left(\frac{P_s |h_{\mathrm{SE}}|^2}{\sum_{n=1}^{N/2} \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n + \delta^2} \geqslant \gamma \right) \\ &= \mathrm{E}_{\boldsymbol{h}_{REn}} \left[P_{h_{\mathrm{SE}}} \left(\frac{P_s |h_{\mathrm{SE}}|^2}{\sum_{n=1}^{N/2} \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n + \delta^2} \geqslant \gamma | \boldsymbol{h}_{REn} \right) \right] \\ &= \mathrm{e}^{\frac{\gamma\delta^2 d_{\mathrm{SE}}^c}{P_s}} \prod_{n=1}^{N/2} \mathrm{E}_{\boldsymbol{h}_{REn}} \left[\mathrm{e}^{-\frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n} \right]. \end{aligned} \tag{22}$$

同样利用文献 [18] 中的式 (14) 的结果, 式 (22) 中的期望可以计算如下:

$$\begin{aligned} \mathrm{E}_{\boldsymbol{h}_{REn}} \left[\mathrm{e}^{-\frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}_n^{\mathrm{H}} \boldsymbol{H}_{REn} \boldsymbol{w}_n} \right] &= \frac{1}{1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \boldsymbol{w}_n^{\mathrm{H}} \mathrm{E}\left(\boldsymbol{H}_{REn}\right) \boldsymbol{w}_n} \\ &= \frac{1}{1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \left(d_{R_{n1} E}^{-c} |w_{n,1}|^2 + d_{R_{n2} E}^{-c} |w_{n,2}|^2 \right)}. \end{aligned} \tag{23}$$

综合式 (22) 和 (23) 中的结果, 可以得到概率 P_2 的最终表达式为

$$P_2 = \frac{\mathrm{e}^{\frac{\gamma\delta^2 d_{\mathrm{SE}}^c}{P_s}}}{\prod_{n=1}^{N/2} \left(1 + \frac{\gamma d_{\mathrm{SE}}^c}{P_s} \left(d_{R_{n1} E}^{-c} |w_{n,1}|^2 + d_{R_{n2} E}^{-c} |w_{n,2}|^2 \right) \right)}. \tag{24}$$

从式 (24) 的分母可以看出, 若 $|w_{n,1}|^2$ 和 $|w_{n,1}|^2$ 越大, 则 P_2 越小. 也就是说在满足迫零准则前提下, 每个协作节点利用的阻塞功率越多, 窃听用户节点的信噪比低于某个给定值的概率越低. 这个结果进一步验证了分组策略算法的正确性. 另外比较式 (21) 和 (24) 的分母可以看出, 由于式 (24) 的分母为 $N/2$ 项的乘积, 展开时包含很多交叉项, 即便是式 (21) 和 (24) 中每个协作节点实际利用的阻塞功率一样大, 式 (24) 中的分母肯定要大于式 (21) 的分母. 实际上分组策略中, 协作节点利用的阻塞功率要大于传统协作干扰策略. 由此一定满足 $P_2 < P_1$. 这也说明了分组协作干扰能更可靠的降低窃听节点的信噪比, 也从另外一个方面证明了分组协作干扰策略要优于传统协作干扰策略.

4 仿真实验与结果

4.1 通信场景

通信场景示意图如图 2 所示. 网络中所有的节点分布在单位距离为 d 的 2 维平面上, 节点的位置与二维平面的坐标一一对应. 假设源节点 S 的坐标固定为 (0,0), 目的节点 D 的坐标固定为 (1,0), 窃

https://engine.scichina.com/doi/10.1360/N112014-00048

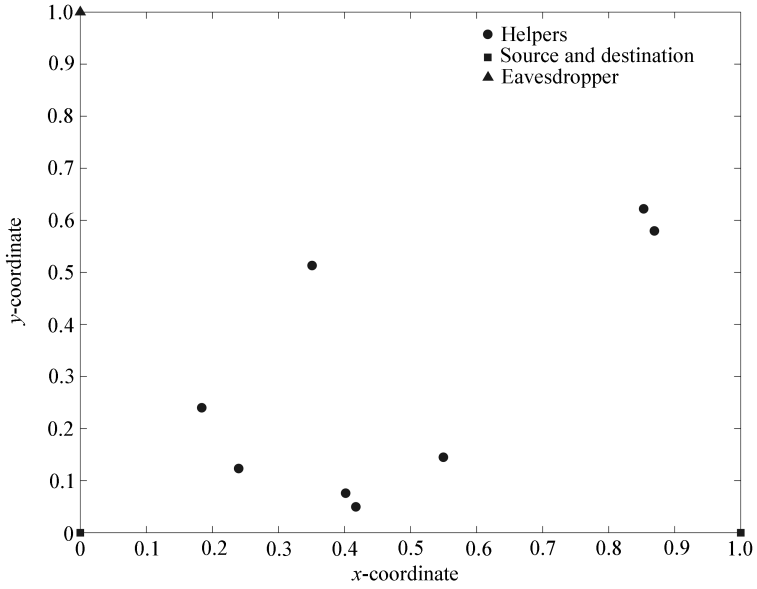


图 2　通信场景

Figure 2　Communication scenario

听节点 E 的坐标固定为 (0,1). N 个协作节点均匀分布在 $d \times d$ 的二维区域内, 每个协作节点的横坐标和纵坐标都大于 0 而小于 1. 在仿真中, 单位距离 d 固定为 20 m, 协作节点个数 N 固定为 8.

4.2　仿真结果

仿真中, 信道的小尺度衰落都是随机产生的独立同分布的零均值单位方差的复高斯随机变量. 节点之间的距离由图 2 中的坐标确定, 路径损耗指数 c 固定为 3.5. 节点处的热噪声功率 $\delta^2 = -60$ dBm, 节点发送私密信号的功率 $P_s = 10$ dBm, 节点发送人工噪声的功率 $P_z \in [-20\ \text{dBm}, 20\ \text{dBm}]$. 对于每一种波束形成系数策略, 均做 1000 次独立的 Monto Carlo 实验, 利用平均安全信息速率衡量不同策略的性能. 仿真中使用 CVX 1.22 软件求解 SDP 优化问题.

在仿真实验中, 首先验证了不同策略对应的平均安全速率随协作节点最大发射功率变化的曲线. 从图 3 可以看出, 随着协作节点最大发射功率的增大, 三种策略的平均安全速率均随之增大, 而且当 $P_z > 10$ dBm 时, 平均安全速率达到一个饱和值. 从式 (5) 和 (12) 很容易看到, 当 P_z 很大的时候, 此时窃听用户端的安全信息速率趋近于零, 则目的节点的安全信息速率趋近于无窃听时的信息速率. 从图 3 可以看出, 最小距离法分组干扰策略要优于固定分组干扰与全体干扰策略. 原因在于前者能更有效的利用阻塞功率. 这个结果从图 4 可以得到进一步的验证.

在未知窃听用户实时信道的情况下, 考虑独立功率约束, 传输策略的优化目标为最大化发射人工噪声的总功率. 图 4 给出了不同传输策略协作节点实际利用的阻塞总功率与节点最大发射功率的关系. 为了便于比较, 图 4 只给出了 P_z 在区间 $[-20\ \text{dBm}, 0\ \text{dBm}]$ 内的功率曲线. 从图 4 中可以明显看出, 最小距离法分组干扰策略利用的阻塞总功率最大, 接近于协作节点可利用的总阻塞功率. 其他两种安全传输策略的阻塞功率利用率相差不大. 最小距离分组干扰策略利用的阻塞总功率最大, 对应于最大的平均安全速率. 一方面验证了在未知窃听用户信道的情况下, 最大化协作节点发射人工噪声的总功率对应于高的安全传输速率. 另一方面也验证了分组协作干扰策略相比传统协作干扰策略, 能更有

https://engine.scichina.com/doi/10.1360/N112014-00048

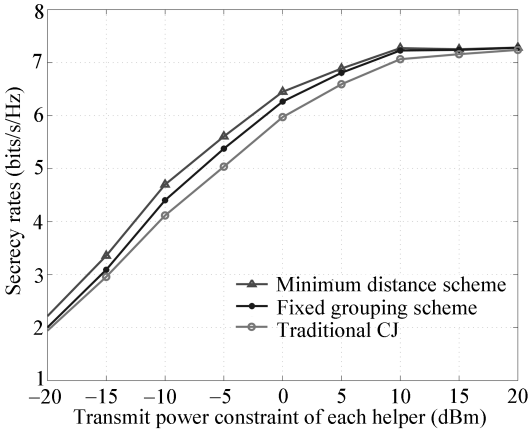


图 3 平均安全速率随协作节点最大发射功率变化曲线

Figure 3 Average secrecy rate vs. transmit power constraint of each helper

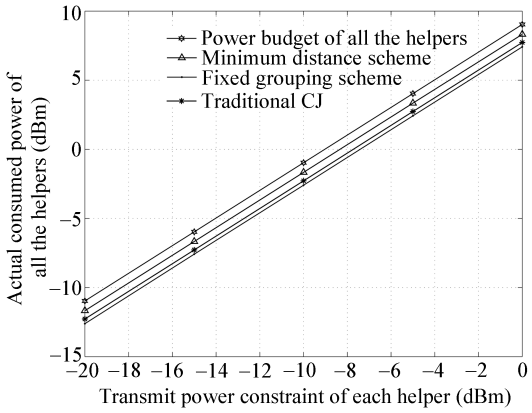


图 4 协作干扰实际利用的总功率随协作节点最大发射功率的变化曲线

Figure 4 Practically consumed total power vs. transmit power constraint of each helper

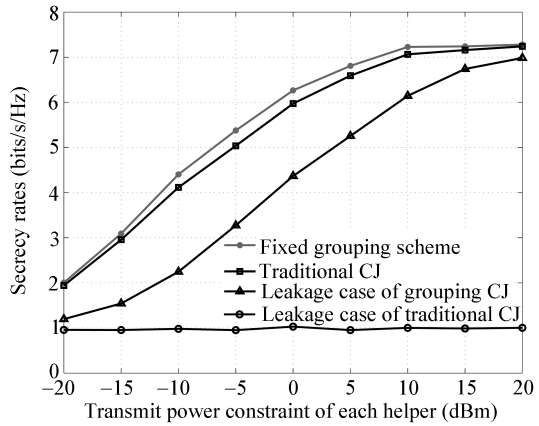


图 5 人工噪声泄露情况下平均安全速率随协作节点最大发射功率的变化曲线

Figure 5 Average secrecy rate vs. transmit power constraint of each helper under artificial noise leakage

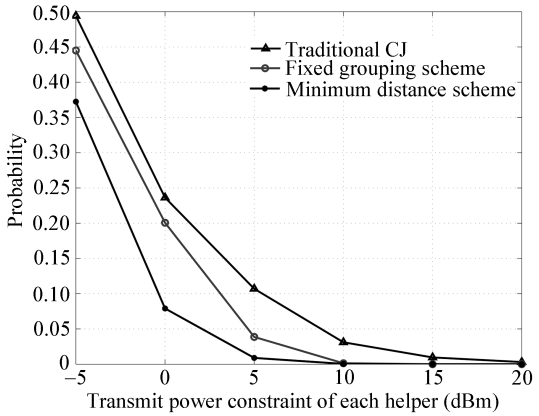


图 6 窃听节点信噪比高于某给定值的概率随协作节点最大发射功率的变化曲线

Figure 6 Probability of those SNR at the eavesdropper beyond a specific threshold vs. transmit power constraint of each helper

效的利用阻塞功率.

在图 5 中, 考虑了人工噪声泄露的情况. 为了比较的公平, 分组策略采用固定分组, 且假设离窃听节点相对距离较近的三组都发生了人工噪声泄露. 此时 4 组干扰中仅有一组工作. 从图 5 可以看到, 当传统协作干扰策略发生人工噪声泄露时, 性能下降很严重. 而对分组协作干扰策略来说, 尽管只有一组协作干扰仍然有效, 性能下降却不是很大, 而且能保证平均安全速率依然随协作节点最大发射功率变大而变大. 这既验证了分组协作干扰传输策略更鲁棒, 也暗示了当人工噪声发生泄露时, 分组策略可以牺牲功率换取高的安全速率.

在图 6 中, 分别比较了三种协作干扰策略中概率 $\mathbb{P}(\Gamma_E \geqslant \gamma)$ 的变化曲线, 其中 $\gamma = 0$ dB. 从图中

https://engine.scichina.com/doi/10.1360/N112014-00048

可以清楚地看到, 随着协作节点的最大发射功率增加, 三种策略中窃听节点信噪比高于 0 dB 的概率逐渐变小. 另外还可以看到相比于传统的协作干扰策略, 两种分组协作干扰的 $\mathbb{P}(\Gamma_E \geqslant \gamma)$ 要更小一些. 特别是当 $P_z > 10$ dBm 时, 分组协作干扰的概率近乎趋近于零. 这说明了分组协作干扰对窃听节点信噪比的损害程度更严重一些, 同时这也验证了式 (21) 和 (24) 中的结论.

5 结论

本文考虑了利用多节点协作干扰增强无线通信安全的问题, 提出了一种新的安全传输策略. 在考虑到传统的协作干扰策略不能充分利用每个节点的阻塞功率和人工噪声可能存在泄露的情况下, 提出了分组协作干扰策略, 并给出了最小距离分组和固定分组两种分组策略. 实验结果验证了在迫零准则下, 最小距离分组协作干扰是最优的安全传输策略. 除此之外, 文章还考虑了人工噪声发生泄露对安全策略性能的影响. 在人工噪声发生泄露的情况下, 分组协作干扰策略性能下降不明显, 而传统协作干扰策略完全失效. 此时分组协作干扰可以利用功率换取高的安全速率. 以上两个方面的结果证实了分组协作干扰策略要优于传统协作干扰策略.

参考文献

1 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inf Theory, 2008, 54: 2515–2534

2 Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process, 2010, 58: 1875–1888

3 Wang H M, Yin Q Y, Xia X G. Distributed beamforming for physical-layer security of two-way relay networks. IEEE Trans Signal Process, 2012, 60: 3532–3545

4 Zheng G, Choo L C, Wong K K. Optimal cooperative jamming to enhance physical layer security using relays. IEEE Trans Signal Process, 2011, 59: 1317–1322

5 Luo M, Wang H M, Yin Q Y. Hybrid relaying and jamming for wireless physical layer security based on cooperative beamforming. Sci Sin Inf, 2013, 43: 445–458 [罗苗, 王慧明, 殷勤业. 基于协作波束形成的中继阻塞混合无线物理层安全传输. 中国科学: 信息科学, 2013, 43: 445–458]

6 Lai L, El Gamal H. The relay-eavesdropper channel: cooperation for secrecy. IEEE Trans Inf Theory, 2008, 54: 4005–4019

7 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1367

8 Luo S, Li J, Petropulu A P. Uncoordinated cooperative jamming for secret communications. IEEE Trans Inf Foren Sec, 2013, 8: 1081–1090

9 Dehghan M, Goeckel D L, Ghaderi M, et al. Energy efficiency of cooperative jamming strategies in secure wireless networks. IEEE Trans Wirel Commun, 2012, 11: 3025–3029

10 Zhou X, McKay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Trans Veh Tech, 2010, 59: 3831–3842

11 Liu Y, Li J, Petropulu A P. Destination assisted cooperative jamming for wireless physical-layer security. IEEE Trans Inf Foren Sec, 2013, 8: 682–694

12 Park K H, Wang T, Alouini M S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. IEEE J Sel Area Commun, 2013, 31: 1741–1750

13 Zhang J, Gursoy M C. Collaborative relay beamforming for secure broadcasting. In: Proceedings of the IEEE Wireless Communications and Networking Conference, Sydney, 2010. 1–6

14 Lin M, Ge J, Yang Y. An effective secure transmission scheme for AF relay networks with two-hop information leakage. IEEE Commun Lett, 2013, 17: 1676–1679

15 Wang H M, Luo M, Xia X G, et al. Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI. IEEE Signal Process Lett, 2013, 20: 39–42

https://engine.scichina.com/doi/10.1360/N112014-00048

16 Luo Z Q, Ma W K, So A M C, et al. Semidefinite relaxation of quadratic optimization problems: from its practical deployments and scope of applicability to key theoretical results. IEEE Signal Process Mag, 2010, 27: 20–34
17 Zhang R, Song L, Han Z, et al. Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans Veh Tech, 2012, 61: 3693–3704
18 Turin G L. The characteristic function of hermitian quadratic forms in complex normal variables. Biometrika, 1960, 47: 199–201

Grouping cooperative jamming for wireless physical layer security

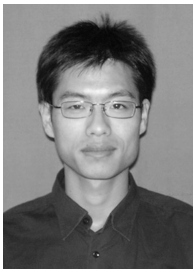
DENG Hao[1,2], WANG HuiMing[1*] & WANG WenJie[1]

1 *School of Electronic and Information Engineering, Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an* 710049*, China*;
2 *School of Physics and Electronics, Henan University, Kaifeng* 475004*, China*
*E-mail: hmwang@mail.xjtu.edu.cn

Abstract In this paper, we propose a novel scheme of grouping cooperative jamming (CJ) for secure communication. During the data transmission, the source broadcasts its information signal, all the helpers simultaneously transmit common artificial noise (AN) to interfere the eavesdropper for tradition CJ. In our scheme, all the helpers are divided to different groups which transmit independent artificial noises to the potential eavesdropper. The zero-forcing beamfomer is selected to cancel the AN out at the destination. The tradition CJ scheme can not completely consume the total power budget, while the grouping scheme is based on the instantaneously channel gain which can make best of the total power per group. The simulations show that our propose scheme based on minimum distance achieves the highest secrecy rate and the power actual consumed approaches to the total power budget. Additionally, we propose a fixed grouping scheme based on the second-order statistics of the channel gain which can be easily implemented. Furthermore, we consider the case that the eavesdropper has knowledge of the artificial noise. The tradition CJ does not work in such case, while our scheme works well even only one group keeps its AN secret. The analytical results and simulations show our scheme achieves better performance than the tradition CJ.

Keywords physical layer security, cooperative jamming, cooperative communication, artificial noise, grouping cooperative

https://engine.scichina.com/doi/10.1360/N112014-00048



DENG Hao was born in 1982. He received the B.S., M.S. degree from Harbin University of Science and Technology, Harbin, in 2004 and 2007, respectively. He is a Ph.D. candidate in Xi'an Jiaotong University and also a lecturer in the School of Physics and Electronics, Henan University, Kaifeng. His research interests include cooperative communications and physical layer security.



WANG WenJie was born in 1970. He received the B.S., M.S., and Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, Xi'an, in 1993, 1998, and 2001, respectively. Currently, he is a professor of Xi'an Jiaotong University. His main research interests include MIMO and OFDM systems, digital signal processing and wireless sensor networks.



WANG HuiMing was born in 1983. He received the B.S. and Ph.D. degree, both in electrical engineering from Xi'an Jiaotong University, Xi'an, in 2004 and 2010, respectively. He is currently an associate professor of the Department of Information and Communications Engineering, Xi'an Jiaotong University, and also working in the Ministry of Education Key Lab for Intelligent Networks and Network Security, China. His research interests include cooperative communication systems, physical-layer security of wireless communications and signal processing for broadband wireless communications.

https://engine.scichina.com/doi/10.1360/N112014-00048