

大规模 MIMO 中继系统中 多用户物理层安全传输方案

雷维嘉,王娟兵,谢显中

(重庆邮电大学通信与信息工程学院,重庆 400065)

摘要: 研究大规模多输入多输出中继网络中的多用户物理层安全传输方案. 系统模型中假设窃听节点与源节点和中继节点间都有直接链路,窃听节点可以接收到源节点和中继发送的信号. 在不能获得窃听者信道状态信息的情况下,大规模 MIMO 中继采用简单的最大比合并/最大比发射信号处理方案,并配合中继零空间人工噪声和目的端的协作干扰实现多用户的信息安全传输. 对保密速率及其在中继天线数无限增长时的渐近值进行了理论分析,并进行仿真. 仿真结果显示系统的保密和速率随中继天线数的增长而增长,最终趋于理论渐近上界值. 仿真结果也表明即使窃听节点具有多用户间干扰消除能力,并能同时拦截源节点和中继发送的信号,采用本文的方案仍然能获得可观保密速率.

关键词: 大规模 MIMO; 中继; 多用户; 物理层安全

中图分类号: TN925 **文献标识码:** A **文章编号:** 0372-2112 (2018)12-2878-10

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.3969/j.issn.0372-2112.2018.12.009

Security Transmission Scheme on Physical Layer for Multi-user in Massive MIMO Relay System

LEI Wei-jia, WANG Juan-bing, XIE Xian-zhong

(School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: The multi-user security transmission scheme on physical layer in a massive multiple-input multiple-output (MIMO) relay based network is studied. There are direct links between the eavesdropper and the source nodes and between the eavesdropper and the relay nodes, so the eavesdropper can receive the signals sent by the source nodes and the relay. The relay employs simple maximum ratio combining in the first stage and maximum ratio transmitting in the second stage by using this scheme and assisted by the null-space artificial noise sent by the relay and the collaboration interference sent by the destination node, security transmission of information between the multi user-pairs is realized even though the channel state information of the eavesdropper cannot be obtained. The secrecy rate and its asymptotic value when the number of antennas of the relay grows to infinity are analyzed. The simulation results show that the secrecy sum rate of the system increases with the number of relay antenna, and eventually reaches the asymptotic value. Furthermore, a considerable secrecy rate can be achieved even if the eavesdropper has the capability to cancel the multi-user interference and to intercept the signals sent by the source nodes and the relay.

Key words: massive MIMO; relay; multi-user; physical layer security

1 引言

由于无线信道的广播特性和无线终端的移动性,无线通信中信息传输的安全性面临更加严峻的挑战.

研究表明,除了传统的密钥加密方法外,物理层安全是另一种实现安全传输的方法^[1]. 无线通信系统中的物理层安全常用的方法是采用波束赋形和人工噪声(Artificial Noise, AN)技术. 多天线的波束赋形技术通过利用

收稿日期:2017-05-16;修回日期:2018-01-18;责任编辑:梅志强

基金项目:国家自然科学基金(No. 61471076);重庆市教委科学技术研究项目(No. KJ1600413);重庆市基础研究与前沿探索项目(No. cstc2018JCYJAX4032)

系统的空间自由度来削弱窃听者对信号的拦截能力,具备多天线的发送端可以对发送信号进行波束赋形^[2],将发射信号波束对准合法用户的方向,零陷对准窃听者,在提高合法接收端接收信号功率同时降低窃听端的接收功率.文献[3]研究了多输入单输出信道下,存在窃听者时无线信息与能量同传的安全波束赋形设计,在保密速率和能量收集约束下,联合优化发射波束赋形矢量、人工噪声协方差和功率分裂因子以最小化发射总功率.人工噪声技术通过在发射信号中加入适当的噪声,保证在合法用户不受很大影响的同时干扰窃听者,从而提高合法用户的安全通信性能.根据发送端是否已知窃听信道状态信息(Channel State Information, CSI)采用不同的人工噪声方案.当发送端未知窃听端 CSI,通常设计 AN 各向同性,均匀分布在合法信道零空间^[4].当发送端已知完整、准确的窃听信道的 CSI 时,通常是联合优化信息和 AN 协方差,从而实现安全通信^[5].由于传统 AN 无法增强合法用户可靠性,针对此问题,文献[6]提出一种新型动态 AN 生成方法,有效提升合法用户性能.

多天线技术中的多输入多输出(Multiple Input Multiple Output, MIMO)技术是在发送端和接收端使用多根天线的通信技术.当收发天线数目达到几百上千根时,收发天线间信道的小尺度衰落会呈现出渐进正交的特性^[7].天线数达到一定规模的系统被称为大规模 MIMO (Massive MIMO) 系统.大规模 MIMO 具有显著提升系统能量效率和频谱效率的优点,信道的渐进正交特性使得基站采用简单的处理即可降低小区间和用户间干扰^[8].由于大规模 MIMO 系统具有丰富的空间自由度,从信息论安全角度研究利用其实现物理层安全传输也具有很大的潜力,目前已有一些文献对此进行了研究.文献[9]给出了多小区大规模 MIMO 系统中存在被动窃听者时的信息安全传输方案,讨论了在完美 CSI 和存在导频污染两种情况下系统的遍历保密速率和保密中断容量.文献[10]讨论了大规模 MIMO 系统中同时存在多个干扰者和一个窃听者的物理层安全问题,基于发射信号矢量和用户功率博弈论提出了一种提高系统保密速率的迭代算法.

利用中继技术,可实现系统容量的提高和覆盖范围的扩大,而大规模 MIMO 中继传输技术对系统性能的改善更为明显.如文献[11]讨论了多用户对通过大规模 MIMO 中继进行通信时的频谱效率,利用大数定律推导了频谱效率的闭式表达式,证明在系统频谱效率保持不变的情况下,源端和中继的功率可以随着中继天线数的增加而减少.而在物理层安全中利用大规模 MIMO 中继,也可明显提高安全传输性能.文献[12]讨论了一对用户通过大规模 MIMO 中继进行通信,同时存在

一个被动窃听者时系统的安全性能.文献对中继采用放大转发和解码转发两种中继模式下的系统保密性能进行了分析和比较,从保密性能和实现复杂度的角度考虑,得出放大转发方式优于解码转发方式的结论.大规模 MIMO 系统的优势在于可同时同频服务多对用户,提高系统容量,因此针对大规模 MIMO 中继同时为多用户提供服务时的安全问题的研究更有实际价值.文献[13]考虑大规模 MIMO 节点同时为多个单天线用户对提供中继转发服务时的物理层安全问题,研究源端和中继功率增加时系统的安全性能的变化情况,结果显示系统安全性存在一个上界,并不会随发送功率的增加而持续增加.

现有的关于大规模 MIMO 中继系统中物理层安全问题的研究中,假设窃听节点仅可以窃听到中继发送的信息,而不能窃听到源节点发送的信息.按这种场景设计的安全方案的限制了窃听者的位置.本文考虑窃听节点能接收到中继节点发送信号,也能接收到源节点发送信号的场景,研究在不能获得窃听者 CSI 情况下,利用大规模 MIMO 中继的多天线自由度和人工噪声实现多对用户间保密信息安全传输的机制.采用由目的节点的协作干扰和中继节点的人工噪声保护第一跳和第二跳中传输的信息的方案,并对一定中继天线数量下系统的保密性能,以及中继节点天线数无限增长时的系统渐近保密性能进行分析.

2 系统模型

K 个单天线源节点(Source Users, SU)与相应的 K 个单天线的目的节点(Destination Users, DU)通过一个装备 $N(N \gg K)$ 根天线的大规模 MIMO 中继(Relay, R)进行通信.每个源节点向一个目的节点发送信息,称为一个用户对.源节点与目的节点不存在直接链路,通过大规模的 MIMO 中继节点转发实现 K 个用户对间在同时同频资源下的并行通信.存在单天线的窃听节点(Eavesdropper, E),与源节点和中继节点间存在链路.假设所有节点每根天线处的信道噪声均是均值为 0、方差为 σ^2 的复高斯白噪声.系统模型如图 1 所示.

记 K 个源端与中继间的信道矩阵为 $\mathbf{G}_1 = \mathbf{H}_1 \mathbf{D}_1^{1/2} \in \mathbb{C}^{N \times K}$, 中继与 K 个目的端间的信道矩阵为 $\mathbf{G}_2 = \mathbf{D}_2^{1/2} \mathbf{H}_2 \in \mathbb{C}^{K \times N}$, 其中 $\mathbf{H}_1 \in \mathbb{C}^{N \times K}$ 和 $\mathbf{H}_2 \in \mathbb{C}^{K \times N}$ 为小尺度衰落,其元素为独立同分布的随机变量,均服从均值为 0、方差为 1 的复高斯分布; \mathbf{D}_1 和 \mathbf{D}_2 是 $K \times K$ 的实对角矩阵,表示大尺度衰落,对角线上的元素 $[\mathbf{D}_1]_{kk} = \eta_{1k}$ 为第 k 个源端到中继的大尺度衰落, $[\mathbf{D}_2]_{kk} = \eta_{2k}$ 为中继到第 k 个目的端的大尺度衰落.

记窃听端与源端、中继、目的端间信道矢量分别为 $\mathbf{f}_{SE} = \mathbf{D}_{SE}^{1/2} \mathbf{f}_{SE} \in \mathbb{C}^{K \times 1}$, $\mathbf{f}_{RE} = \mathbf{D}_{RE}^{1/2} \mathbf{f}_{RE} \in \mathbb{C}^{N \times 1}$ 和 $\mathbf{f}_{DE} = \mathbf{D}_{DE}^{1/2} \mathbf{f}_{DE} \in$

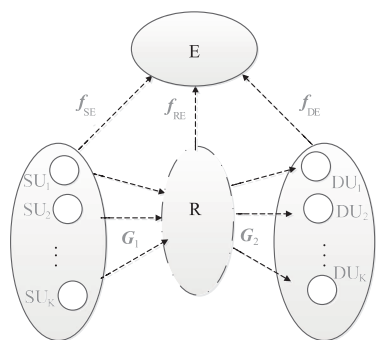


图1 系统模型

$\mathbb{C}^{K \times 1}$. 其中 $\mathbf{f}_{SE} \in \mathbb{C}^{K \times 1}$, $\mathbf{f}_{RE} \in \mathbb{C}^{N \times 1}$ 和 $\mathbf{f}_{DE} \in \mathbb{C}^{K \times 1}$ 为小尺度衰落, 其元素为独立同分布的随机变量, 服从均值为 0、方差为 1 的复高斯分布; \mathbf{D}_{SE} 、 \mathbf{D}_{DE} 是 $K \times K$ 的实对角矩阵, D_{RE} 为实数, 分别表示窃听端与源端、目的端、中继的大尺度衰落. 考虑窃听节点为被动节点的场景, 合法节点不能获得窃听节点各信道的状态信息.

采用放大转发中继辅助的两跳传输方案, 中继采用时分双工模式. 第 1 跳, 源节点发送信号到中继, 为避免窃听节点获取源节点发送的信息, 目的节点同时发送人工噪声来干扰窃听器. 中继节点接收到的信号为

$$\mathbf{y}'_R = \sqrt{P_S} \mathbf{G}_1 \mathbf{x} + \sqrt{P_{nd}} \mathbf{G}_2^T \mathbf{z}_D + \mathbf{n}_R \quad (1)$$

式中: 上标 T 表示矩阵的转置; P_S 是每个源节点发送信号的功率, $\mathbf{x} = [x_1, x_2, \dots, x_K]^T$ 是 K 个源节点发送信号构成的矢量, 满足 $E[|x_k|^2] = 1, i = 1, 2, \dots, K$; P_{nd} 是每个目的节点发送人工噪声的功率; $\mathbf{z}_D \sim \mathcal{CN}(0, \mathbf{I}_K)$ 是 K 个目的节点随机生成的人工噪声构成的矢量; $\mathbf{n}_R \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_N)$ 是中继节点处的复加性高斯白噪声矢量. 其中, \mathbf{I}_A 表示 $A \times A$ 阶单位矩阵.

中继节点采用最大比合并 (Maximum Ratio Combining, MRC) 接收信号, 其最大比合并矩阵为

$$\mathbf{W}_R = \mathbf{G}_1^H \quad (2)$$

其中, 上标 H 表示矩阵的共轭转置. 合并后中继的接收信号为

$$\begin{aligned} \mathbf{y}_R &= \mathbf{W}_R \mathbf{y}'_R = \mathbf{G}_1^H (\sqrt{P_S} \mathbf{G}_1 \mathbf{x} + \sqrt{P_{nd}} \mathbf{G}_2^T \mathbf{z}_D + \mathbf{n}_R) \\ &= \sqrt{P_S} \mathbf{G}_1^H \mathbf{G}_1 \mathbf{x} + \sqrt{P_{nd}} \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D + \mathbf{G}_1^H \mathbf{n}_R \end{aligned} \quad (3)$$

第 2 跳, 中继对接收信号进行放大转发, 转发的信号为经过最大比发射 (Maximum Ratio Transmission, MRT) 预编码后的信号. 由于没有窃听信道的状态信息, 采用发送 \mathbf{G}_2 零空间上的人工噪声的方式干扰窃听节点, 降低窃听节点解码信号的能力. 发送的信号为

$$\mathbf{x}_R = \alpha \mathbf{W}_T \mathbf{y}_R + \sqrt{P_{nr}} \mathbf{V}_2 \mathbf{z}_R \quad (4)$$

式中: α 为中继放大转发系数, 满足中继发送功率的限制; P_{nr} 是中继每根天线上发送人工噪声的平均功率; \mathbf{W}_T 为中继发送信号预编码矩阵; \mathbf{z}_R 是服从复高斯分布

的 $N-K$ 维人工噪声矢量, $\mathbf{z}_R \sim \mathcal{CN}(0, \mathbf{I}_{N-K})$; \mathbf{V}_2 是中继人工噪声波束赋形矩阵. \mathbf{W}_T 为

$$\mathbf{W}_T = \mathbf{G}_2^H \quad (5)$$

人工噪声波束赋形矩阵 \mathbf{V}_2 使人工噪声位于主信道 \mathbf{G}_2 的零空间上, 不对目的端的接收造成影响, 即

$$\mathbf{G}_2 \mathbf{V}_0 = 0, \mathbf{V}_2 = \frac{\mathbf{V}_0}{\sqrt{\text{Tr}(\mathbf{V}_0 (\mathbf{V}_0^H))}} \quad (6)$$

其中, $\mathbf{V}_0 \in \mathbb{C}^{N \times (N-K)}$ 是主信道零空间的投影矩阵, 它的功率归一化形式为 $\mathbf{V}_2 \in \mathbb{C}^{N \times (N-K)}$; $\text{Tr}(\mathbf{A})$ 为矩阵 \mathbf{A} 的迹.

目的节点接收到的中继转发信号为

$$\mathbf{y}_D = \mathbf{G}_2 \mathbf{x}_R + \mathbf{n}_D \quad (7)$$

上式, $\mathbf{n}_D \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_K)$ 为目的节点复加性高斯白噪声矢量.

窃听端第 1 跳中接收到的信号为

$$y_E^{(1)} = \sqrt{P_S} \mathbf{f}_{SE}^T \mathbf{x} + \sqrt{P_{nd}} \mathbf{f}_{DE}^T \mathbf{z}_D + n_E^{(1)} \quad (8)$$

第 2 跳中接收到的信号为

$$y_E^{(2)} = \mathbf{f}_{RE}^T \mathbf{x}_R + n_E^{(2)} \quad (9)$$

式中, $n_E^{(1)} \sim \mathcal{CN}(0, \sigma^2)$, $n_E^{(2)} \sim \mathcal{CN}(0, \sigma^2)$ 分别为窃听节点处第 1 跳和第 2 跳的复加性高斯白噪声. 本文中, 符号上标 (1)、(2) 分别表示第 1 跳和第 2 跳.

3 保密速率分析

3.1 保密速率分析

将式(3)和式(5)代入式(4), 可得中继在第 2 跳中发送的信号为

$$\begin{aligned} \mathbf{x}_R &= \alpha \mathbf{W}_T \mathbf{W}_R (\sqrt{P_S} \mathbf{G}_1 \mathbf{x} + \sqrt{P_{nd}} \mathbf{G}_2^T \mathbf{z}_D + \mathbf{n}_R) + \sqrt{P_{nr}} \mathbf{V}_2 \mathbf{z}_R \\ &= \alpha \sqrt{P_S} \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_1 \mathbf{x} + \alpha \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R \\ &\quad + \alpha \sqrt{P_{nd}} \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D + \sqrt{P_{nr}} \mathbf{V}_2 \mathbf{z}_R \end{aligned} \quad (10)$$

在中继节点每根天线的平均发送总功率为 P_R 、人工噪声平均功率为 P_{nr} 时, 转发源端信号的平均功率为 $P_R - P_{nr}$, 在此约束下, 中继的放大系数为

$$\alpha = \sqrt{\frac{P_R - P_{nr}}{P_S \text{Tr}(\mathbf{A}_1) + \sigma^2 \text{Tr}(\mathbf{A}_2) + P_{nr} \text{Tr}(\mathbf{A}_3)}} \quad (11)$$

式中 $\mathbf{A}_1 = \mathbf{G}_2 \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_1 \mathbf{G}_1^H \mathbf{G}_1$, $\mathbf{A}_2 = \mathbf{G}_2 \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_1$, $\mathbf{A}_3 = \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{G}_2^*$ 上标 * 表示取共轭.

把式(10)代入式(7), 可得 K 个目的节点的接收信号构成的矢量为

$$\begin{aligned} \mathbf{y}_D &= \alpha \sqrt{P_S} \mathbf{G}_2 \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_1 \mathbf{x} + \alpha \mathbf{G}_2 \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R \\ &\quad + \alpha \sqrt{P_{nd}} \mathbf{G}_2 \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D + \sqrt{P_{nr}} \mathbf{G}_2 \mathbf{V}_2 \mathbf{z}_R + \mathbf{n}_D \end{aligned} \quad (12)$$

其中第 k 个目的节点的接收信号为

$$y_{D,k} = \underbrace{\alpha \sqrt{P_S} \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k} \mathbf{x}_k}_{\text{用户的信号}} + \underbrace{\alpha \sqrt{P_S} \sum_{i=1, i \neq k}^K \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,i} \mathbf{x}_i}_{\text{其他用户的信号}}$$

$$\begin{aligned}
& + \alpha \sqrt{P_{\text{nd}}} \underbrace{\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D}_{\text{目的节点发送的人工噪声}} + \sqrt{P_{\text{nr}}} \underbrace{\mathbf{g}_{2,k}^T \mathbf{V}_2 \mathbf{z}_R}_{\text{中继发送的人工噪声}} \\
& + \alpha \underbrace{\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R}_{\text{中继转发的噪声}} + \underbrace{n_{D,k}}_{\text{噪声}}
\end{aligned} \quad (13)$$

上式中, x_k 是第 k 个源节点发送的信号, \mathbf{g}_{2k} 是 \mathbf{G}_2^T 的第 k 列向量, \mathbf{g}_{1k} 是 \mathbf{G}_1 的第 k 列向量. 等式右边第 1 项为期望发送给目的用户 k 的信号, 第 2 项为其他用户的干扰, 第 3 项为目的节点发送人工噪声, 第 4 项为中继节点发送的人工噪声, 第 5 项为中继节点转发的信道噪声, 最后一项为目的用户 k 接收到的信道噪声. 而中继节点发送的人工噪声位于 \mathbf{G}_2 的零空间中, 因此第 4 项为零. 因此, 第 k 个目的节点的接收信干噪比 (Signal to Interference-Noise Ratio, SINR) 为

$$\begin{aligned}
\gamma_{D,k} &= \\
& \frac{\alpha^2 P_S |\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k}|^2}{\alpha^2 (P_S \sum_{i=1, i \neq k}^K |c_{1,i}|^2 + P_{\text{nd}} \|\mathbf{b}_1\|^2 + \|\mathbf{b}_2\|^2 \sigma^2) + \sigma^2}
\end{aligned} \quad (14)$$

式中, $c_{1,i} = \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,i}$, $\mathbf{b}_1 = \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T$, $\mathbf{b}_2 = \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H$; $|\cdot|$ 表示复数的模; $\|\mathbf{a}\|$ 是向量 \mathbf{a} 的范数.

第 k 个目的节点的可达速率为

$$R_{D,k} = \frac{1}{2} \log_2(1 + \gamma_{D,k}) \quad (15)$$

这里, 产生标量系数 1/2 的原因是采用中继两跳方式传输时, 源和中继各使用一半的信道资源进行传输.

相应的, K 个目的节点可达和速率为

$$R_D = \sum_{k=1}^K R_{D,k} \quad (16)$$

把式(10)带入式(9), 可得窃听节点在第 2 跳中的接收信号为

$$\begin{aligned}
y_{E,k}^{(2)} &= \alpha \sqrt{P_S} \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{x} + \alpha \sqrt{P_{\text{nd}}} \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D \\
& + \sqrt{P_{\text{nr}}} \mathbf{f}_{\text{RE}}^T \mathbf{V}_2 \mathbf{z}_R + \alpha \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R + n_{E,k}^{(2)}
\end{aligned} \quad (17)$$

进一步, 窃听节点要获取第 k 个用户信息时, 可将其在两跳接收信号写为

$$\begin{aligned}
y_{E,k}^{(1)} &= \underbrace{\sqrt{P_S} f_{\text{SE},k} x_k}_{\text{用户 } k \text{ 的信号}} + \underbrace{\sqrt{P_S} \sum_{i=1, i \neq k}^K f_{\text{SE},i} x_i}_{\text{其他用户的信号}} + \underbrace{\sqrt{P_{\text{nd}}} f_{\text{DE}}^T \mathbf{z}_D}_{\text{人工噪声}} + \underbrace{n_{E,k}^{(1)}}_{\text{噪声}}
\end{aligned} \quad (18)$$

$$\begin{aligned}
y_{E,k}^{(2)} &= \alpha \sqrt{P_S} \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k} x_k + \alpha \sqrt{P_S} \underbrace{\sum_{i=1, i \neq k}^K \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,i} x_i}_{\text{其他用户的信号}} \\
& + \alpha \sqrt{P_{\text{nd}}} \underbrace{\mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D}_{\text{目的节点发送的人工噪声}} + \sqrt{P_{\text{nr}}} \underbrace{\mathbf{f}_{\text{RE}}^T \mathbf{V}_2 \mathbf{z}_R}_{\text{中继发送人工噪声}} \\
& + \alpha \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R + \underbrace{n_{E,k}^{(2)}}_{\text{噪声}}
\end{aligned} \quad (19)$$

其中, $f_{\text{SE},k}$ 是 \mathbf{f}_{SE} 的第 k 个元素

窃听节点对多个用户信息的处理我们分两种情况进行讨论. 一种是窃听节点没有用户间干扰消除的能

力; 另一种情况是窃听节点具有用户间干扰消除的能力, 这里考虑对信息保密传输最不利的一种情况, 即窃听者在接收一个用户的信息时, 其他用户的信号其可采用干扰消除技术完全消除. 在下面的讨论中, 我们将两种情况分别用符号 NIC 和 IC 标记.

第一种情况下, 窃听节点获取第 k 个用户的信息时, 两时隙的接收 SINR 分别为

$$\begin{aligned}
\gamma_{E,k}^{(1), \text{NIC}} &= \frac{P_S |f_{\text{SE},k}|^2}{P_S \sum_{i=1, i \neq k}^K |f_{\text{SE},i}|^2 + P_{\text{nd}} \|\mathbf{f}_{\text{DE}}^T\|^2 + \sigma^2}
\end{aligned} \quad (20)$$

$$\begin{aligned}
\gamma_{E,k}^{(2), \text{NIC}} &= \\
& \frac{\alpha^2 P_S |\mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k}|^2}{\alpha^2 (P_S \sum_{i=1, i \neq k}^K |c_{2,i}|^2 + P_{\text{nd}} \|\mathbf{b}_3\|^2 + \|\mathbf{b}_4\|^2 \sigma^2) + P_{\text{nr}} \|\mathbf{b}_5\|^2 + \sigma^2}
\end{aligned} \quad (21)$$

式中, $c_{2,i} = \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,i}$, $\mathbf{b}_3 = \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T$, $\mathbf{b}_4 = \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H$, $\mathbf{b}_5 = \mathbf{f}_{\text{RE}}^T \mathbf{V}_2$.

窃听节点采用最大比合并后接收 SINR 为

$$\gamma_{E,k}^{\text{NIC}} = \gamma_{E,k}^{(1), \text{NIC}} + \gamma_{E,k}^{(2), \text{NIC}} \quad (22)$$

窃听节点窃听所有用户信息的和速率为

$$R_E^{\text{NIC}} = \sum_{k=1}^K \frac{1}{2} \log_2(1 + \gamma_{E,k}^{\text{NIC}}) \quad (23)$$

系统保密和速率为

$$R_S^{\text{NIC}} = \sum_{k=1}^K \left[\frac{1}{2} \log_2(1 + \gamma_{D,k}) - \frac{1}{2} \log_2(1 + \gamma_{E,k}^{\text{NIC}}) \right]^+ \quad (24)$$

其中, $[\lambda]^+ = \max(0, \lambda)$.

系统保密能量效率为

$$\mathcal{E}_S^{\text{NIC}} = \frac{R_S^{\text{NIC}}}{NP_R + KP_S + KP_{\text{nd}}} \quad (25)$$

第二种情况下, 窃听节点获取第 k 个用户的信息时, 两时隙的接收 SINR 分别为

$$\begin{aligned}
\gamma_{E,k}^{(1), \text{IC}} &= \frac{P_S |f_{\text{SE},k}|^2}{P_{\text{nd}} |f_{\text{SE},i}|^2 + \sigma^2}
\end{aligned} \quad (26)$$

$$\begin{aligned}
\gamma_{E,k}^{(2), \text{IC}} &= \frac{\alpha^2 P_S |\mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k}|^2}{\alpha^2 P_{\text{nd}} \|\mathbf{A}_4\|^2 + P_{\text{nr}} \|\mathbf{A}_5\|^2 + \alpha^2 \|\mathbf{A}_6\|^2 \sigma^2 + \sigma^2}
\end{aligned} \quad (27)$$

式中, $\mathbf{A}_4 = \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T$, $\mathbf{A}_5 = \mathbf{f}_{\text{RE}}^T \mathbf{V}_2$, $\mathbf{A}_6 = \mathbf{f}_{\text{RE}}^T \mathbf{G}_2^H \mathbf{G}_1^H$.

窃听节点采用最大比合并后接收 SINR 为

$$\gamma_{E,k}^{\text{IC}} = \gamma_{E,k}^{(1), \text{IC}} + \gamma_{E,k}^{(2), \text{IC}} \quad (28)$$

窃听节点窃听所有用户信息的和速率为

$$R_E^{\text{IC}} = \sum_{k=1}^K \frac{1}{2} \log_2(1 + \gamma_{E,k}^{\text{IC}}) \quad (29)$$

系统保密和速率为

$$R_s^{\text{IC}} = \sum_{k=1}^K \left[\frac{1}{2} \log_2(1 + \gamma_{D,k}) - \frac{1}{2} \log_2(1 + \gamma_{E,k}^{\text{IC}}) \right]^+ \quad (30)$$

系统保密能量效率为

$$\varepsilon_s^{\text{IC}} = \frac{R_s^{\text{IC}}}{NP_R + KP_S + KP_{\text{nd}}} \quad (31)$$

3.2 中继天线数增长时渐近保密速率分析

假设源节点发送信号功率 P_S 和目的节点发送人工噪声功率 P_{nd} 不变, 中继节点发送总功率在天线数变化时不变, 也即 $NP_R = P_{\text{RT}}$ 不变, 每根天线发送人工噪声的平均功率为 $P_{\text{nr}} = \beta P_R = \beta P_{\text{RT}}/N, 0 \leq \beta < 1$ 为人工噪声功率分配比例, 相应, 每根天线转发信号的平均功率为 $(1 - \beta)P_R = (1 - \beta)P_{\text{RT}}/N$.

在发射天线数为 N_t 、接收天线数为 N_r 的大规模 MIMO 系统中, 信道矩阵 $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, 假设其元素为独立同分布的随机变量, 服从均值为 0、方差为 1 的复高斯分布. 当 $N_r \gg N_t$ 时, 信道矩阵的列向量是渐近正交的^[7], 即有

$$(\mathbf{H}^H \mathbf{H} / N_r)_{N_r \gg N_t} = \mathbf{I}_{N_t} \quad (32)$$

当 $N_t \gg N_r$ 时, 信道矩阵的行向量是渐近正交的, 即有

$$(\mathbf{H} \mathbf{H}^H / N_t)_{N_t \gg N_r} = \mathbf{I}_{N_r} \quad (33)$$

在本文的系统模型中, 当中继天线数 $N \rightarrow \infty$ 时, 由于 $K \ll N$, 根据式 (32), 源端到中继间的信道矩阵 \mathbf{G}_1 有以下逼近准则:

$$\frac{\mathbf{G}_1^H \mathbf{G}_1}{N} = \mathbf{D}_1^{1/2} \left(\frac{\mathbf{H}_1^H \mathbf{H}_1}{N} \right)_{N \gg K} \mathbf{D}_1^{1/2} \xrightarrow{N \rightarrow \infty} \mathbf{D}_1 \quad (34)$$

进一步得到

$$\frac{\mathbf{g}_{1,k}^H \mathbf{g}_{1,i}}{N} \xrightarrow{N \rightarrow \infty} 0 (i \neq k), \quad \frac{\mathbf{g}_{1,k}^H \mathbf{g}_{1,i}}{N} \xrightarrow{N \rightarrow \infty} \eta_{1k} (i = k) \quad (35)$$

同样地, 对于中继到目的端的信道矩阵 \mathbf{G}_2 , 根据式 (33) 有以下逼近准则:

$$\frac{\mathbf{G}_2 \mathbf{G}_2^H}{N} = \mathbf{D}_2^{1/2} \left(\frac{\mathbf{H}_2 \mathbf{H}_2^H}{N} \right)_{N \gg K} \mathbf{D}_2^{1/2} \xrightarrow{N \rightarrow \infty} \mathbf{D}_2 \quad (36)$$

$$\frac{\mathbf{g}_{2,k}^T \mathbf{g}_{2,i}^*}{N} \xrightarrow{N \rightarrow \infty} 0 (i \neq k), \quad \frac{\mathbf{g}_{2,k}^T \mathbf{g}_{2,i}^*}{N} \xrightarrow{N \rightarrow \infty} \eta_{2k} (i = k) \quad (37)$$

为了得到 $N \rightarrow \infty$ 时中继放大转发系数, 将式 (11) 改写为

$$\alpha^2 = \frac{(1 - \beta)P_{\text{RT}}}{\left[N^4 P_S \text{Tr} \left(\frac{\mathbf{A}_1}{N^3} \right) + N^3 \sigma^2 \text{Tr} \left(\frac{\mathbf{A}_2}{N^2} \right) + N^4 P_{\text{nd}} \text{Tr} \left(\frac{\mathbf{A}_3}{N^3} \right) \right]} \quad (38)$$

式中, $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$ 的定义同式 (11).

当 N 趋于无穷时, 上式中分母第 1 项中 $\text{Tr}(\mathbf{A}_1/N^3) \rightarrow \text{Tr}(\mathbf{D}_2 \mathbf{D}_1 \mathbf{D}_1)$, 第 2 项中 $\text{Tr}(\mathbf{A}_3/N^3) \rightarrow \text{Tr}(\mathbf{D}_2 \mathbf{D}_1)$, 第 3 项中 $\text{Tr}(\mathbf{A}_3/N^3) \rightarrow 0$, 因为 \mathbf{G}_1 和 \mathbf{G}_2 满足统计独立性, 所以分母的收敛性由 N 的最高次项即第一项决定. 因此

推导可得下式

$$\alpha^2 N^4 \rightarrow \frac{(1 - \beta)P_{\text{RT}}}{P_S \text{Tr}(\mathbf{D}_2 \mathbf{D}_1 \mathbf{D}_1)}, \quad \alpha^2 N^3 \rightarrow 0 \quad (39)$$

为了得到 $N \rightarrow \infty$ 时用户 k 的渐进信干噪比, 将式 (13) 改写为

$$\begin{aligned} y_{D,k} &= \alpha N^2 \sqrt{P_S} \frac{\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,k}}{N^2} x_k \\ &+ \alpha N^2 \sqrt{P_S} \sum_{i=1, i \neq k}^K \frac{\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{g}_{1,i}}{N^2} x_i \\ &+ \alpha \sqrt{P_{\text{nd}}} \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D \\ &+ \alpha \sqrt{N^3} \frac{\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{n}_R}{N \sqrt{N}} + n_{D,k} \\ &= \alpha N^2 \sqrt{P_S} \sum_{i=1}^K \frac{\mathbf{g}_{2,k}^T \mathbf{g}_{2,i}^* \mathbf{g}_{1,i}^H \mathbf{g}_{1,k}}{N^2} x_k \\ &+ \alpha N^2 \sqrt{P_S} \sum_{j=1}^K \sum_{i=1, i \neq k}^K \frac{\mathbf{g}_{2,k}^T \mathbf{g}_{2,j}^* \mathbf{g}_{1,j}^H \mathbf{g}_{1,i}}{N^2} x_i \\ &+ \alpha \sqrt{P_{\text{nd}}} \mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T \mathbf{z}_D \\ &+ \alpha \sqrt{N^3} \sum_{i=1}^K \frac{\mathbf{g}_{2,k}^T \mathbf{g}_{2,i}^* \mathbf{g}_{1,i}^H \mathbf{n}_R}{N \sqrt{N}} + n_{D,k} \end{aligned} \quad (40)$$

根据式 (34) ~ (37) 逼近准则, 上式最后一个等号右边第 1、2 项在 $N \rightarrow \infty$ 时极限值分别为 $\alpha N^2 \sqrt{P_S} \eta_{2k} \eta_{1k} x_k, 0$, 功率值分别为 $\alpha^2 N^4 P_S \eta_{2k}^2 \eta_{1k}^2, 0$, 由式 (39) 可知, 第 1 项的功率值为常数.

式 (40) 中最后一个等号右边第 3 项的功率值为 $\alpha^2 P_{\text{nd}} |\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T|$. 将 α^2 的表达式 (39) 代入, 进一步得其功率值为

$$\frac{N^4 P_{\text{nd}} (1 - \beta) P_{\text{RT}} (|\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T|^2 / N^4)}{N^4 P_S \text{Tr}(\mathbf{A}_1 / N^3) + N^3 \sigma^2 \text{Tr}(\mathbf{A}_2 / N^2) + N^4 P_{\text{nd}} \text{Tr}(\mathbf{A}_3 / N^3)}$$

当中继天线数 N 无线增长时, 式中 $\frac{|\mathbf{g}_{2,k}^T \mathbf{G}_2^H \mathbf{G}_1^H \mathbf{G}_2^T|^2}{n^4}$ 趋于 0, 其余部分收敛为常数, 因此 $N \rightarrow \infty$ 时式 (40) 中第 3 项的功率值为零.

假设 $\mathbf{p} = [p_1, p_2, \dots, p_N]^T, \mathbf{q} = [q_1, q_2, \dots, q_N]^T$ 中的元素是均值为 0、方差分别为 σ_p^2 和 σ_q^2 的、相互独立的复高斯随机变量, 根据 Lindeberg-Levy 中心极限定理^[14], 可知 $\mathbf{p}^H \mathbf{q} \sqrt{N}$ 在 $N \rightarrow \infty$ 时是均值为 0、方差为 $\sigma_p^2 \sigma_q^2$ 的复高斯随机变量. 式 (40) 最后一个等号右边第 4 项中, $\mathbf{g}_{1,i}^H \in \mathbb{C}^{1 \times N}, \mathbf{n}_R \in \mathbb{C}^{N \times 1}$ 满足此定理条件, 因此 $N \rightarrow \infty$ 时 $\mathbf{g}_{1,i}^H \mathbf{n}_R$ 的极限值为 \tilde{n}_R , 其中 $\tilde{n}_R \sim \mathcal{CN}(0, \eta_{1k} \sigma^2)$. 这样式 (40) 最后一个等号右边第 4 项的功率值为 $\alpha^2 N^3 \eta_{2k}^2 \eta_{1k} \sigma^2$, 由式 (39) 可知, 该值为 0.

第 5 项为信道噪声, 与 N 无关, 其功率值为 σ^2 .

这样在 $N \rightarrow \infty$ 时, 用户 k 的接收 SINR 为

$$\hat{\gamma}_{D,k} = \frac{\alpha^2 N^4 \eta_{1k}^2 \eta_{2k}^2 P_S}{\sigma^2} = \frac{(1 - \beta) P_{\text{RT}} \eta_{2k}^2 \eta_{1k}^2}{\sigma^2 \text{Tr}(\mathbf{D}_2 \mathbf{D}_1 \mathbf{D}_1)} \quad (41)$$

K 个目的节点的和速率为

$$\hat{R}_D = \sum_{k=1}^K \frac{1}{2} \log_2 \left[1 + \frac{(1-\beta)P_{RT}\eta_{2k}^2\eta_{1k}^2}{\sigma^2 \text{Tr}(\mathbf{D}_2\mathbf{D}_1\mathbf{D}_1)} \right] \quad (42)$$

窃听节点第 1 跳 SINR 与中 N 无关,不随它的变化而变化. 第 2 跳 SINR 则会在 $N \rightarrow \infty$ 时趋于零, 推导过程如下.

窃听节点第 2 跳接收信号的式 (17) 中, 信号部分为

$$\mathbf{x}_E^{(2)} = \alpha \sqrt{P_{RE}} \mathbf{f}_{RE}^H \mathbf{G}_2 \mathbf{G}_1^H \mathbf{G}_1 \mathbf{x} \quad (43)$$

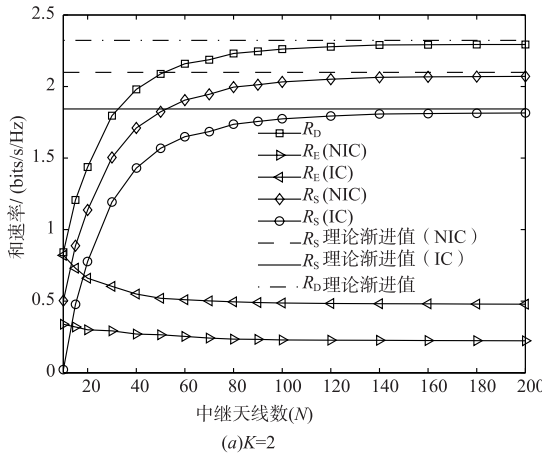
当中继天线数无限增长时, 它的功率值为 $\alpha^2 P_s |\mathbf{f}_{RE}^H \mathbf{G}_2 \mathbf{G}_1^H \mathbf{G}_1|^2$, 将 α^2 的表达式 (39) 代入得它的功率值为

$$\frac{N^4 P_{nd} (1-\beta) P_{RT} (|\mathbf{f}_{RE}^H \mathbf{G}_2 \mathbf{G}_1^H \mathbf{G}_1|^2 / N^4)}{N^4 P_s \text{Tr}(\mathbf{A}_1 / N^3) + N^3 \sigma^2 \text{Tr}(\mathbf{A}_2 / N^2) + N^4 P_{nd} \text{Tr}(\mathbf{A}_3 / N^2)}$$

这里, \mathbf{A}_1 、 \mathbf{A}_2 、 \mathbf{A}_3 的定义同式 (11). 与式 (40) 中等号右边第 3 项分析类似, 可得窃听节点信号部分的功率值趋于零, 即窃听节点在第 2 跳中的接收 SINR 为 0. 因此, $N \rightarrow \infty$ 时, 窃听节点两种用户间干扰处理能力情况下系统可实现保密和速率将分别趋于

$$\hat{R}_S^{\text{NIC}} = \sum_{k=1}^K \left[\frac{1}{2} \log_2 (1 + \hat{\gamma}_{D,k}) - \frac{1}{2} \log_2 (1 + \gamma_{E,k}^{(1),\text{NIC}}) \right]^+ \quad (44)$$

$$\hat{R}_S^{\text{IC}} = \sum_{k=1}^K \left[\frac{1}{2} \log_2 (1 + \hat{\gamma}_{D,k}) - \frac{1}{2} \log_2 (1 + \gamma_{E,k}^{(1),\text{IC}}) \right]^+ \quad (45)$$



4 仿真

本节对提出的方案进行仿真. 仿真中, 假设所有信道都是瑞利衰落信道, 且只考虑小尺度衰落, 即大尺度衰落矩阵 \mathbf{D}_1 、 \mathbf{D}_2 、 \mathbf{D}_{SE} 、 \mathbf{D}_{DE} 均为单位阵, $\mathbf{D}_{RE} = \mathbf{1}$, 各信道增益均为均值为 0、方差为 1 的复高斯分布的随机变量. 所有节点的信道噪声功率均为 $\sigma^2 = 0.01\text{W}$.

图 2 是用户对数 $K=2$ 和 4 时, 用户和速率、窃听节点和速率、系统保密和速率随中继天线数 N 变化的曲线. 仿真中固定设置源节点发送功率 $P_s = 0.1\text{W}$; 中继节点发送总功率 $P_{RT} = NP_R = 0.1\text{W}$, $\beta = 0.2$, 即人工噪声功率 $P_{nr} = 0.2P_R$; 目的节点发送人工噪声功率 $P_{nd} = 0.06\text{W}$. 从仿真结果可以看到, 随着中继天线数的增长, 目的节点可达和速率也在增加, 并趋近于 $N \rightarrow \infty$ 时的理论渐近值; 而窃听节点具有用户间干扰消除能力时的信息拦截速率高于无干扰消除能力时, 且都则随中继天线数的增加而降低, 并趋于一个较小的值; 系统的保密和速率也随中继天线数的增加而增加, 并趋于理论上界值. 用户对数 $K=4$ 时的用户和速率高于 $K=2$ 时, 但前者的速率并不是后者的 2 倍, 可见用户对增加导致用户间干扰增加, 每个用户对速率有所下降, 但系统总的和速率增加. 相应, 用户对数较多时系统的保密和速率也较高. 当窃听节点具备用户间干扰消除能力时, 窃听节点的拦截速率更高, 系统的保密速率较小.

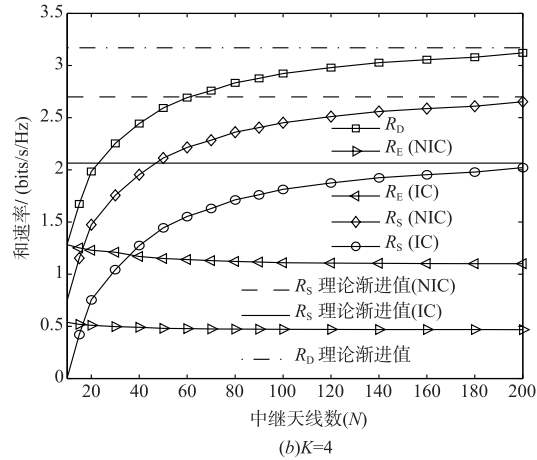


图 2 中继天线数与系统和速率关系

图 3 是中继天线数 $N = 100$ 的情况下, 用户和速率、窃听节点和速率、系统保密和速率随用户对数变化的关系曲线. 仿真中固定设置源节点发送功率 $P_s = 0.1\text{W}$, 中继节点发送总功率 $P_{RT} = NP_R = 0.1\text{W}$, $\beta = 0.3$, 即人工噪声功率 $P_{nr} = 0.3P_R$; 目的节点发送人工噪声功率 $P_{nd} = 0.1\text{W}$. 从仿真结果可以看到, 随着用户对数增长, 目的节点和速率相应增长, 但增长速度逐渐下降. 而对于窃听节点, 即使是在其能消除用户间干扰

的情况下, 其窃听和速率也不能随用户对数的增加而明显增加, 这主要得益于人工噪声对其的干扰, 以及大规模 MIMO 中继所具有的空间选择性. 而在窃听者不能消除用户间的干扰时, 用户对数的增加反而导致窃听和速率下降, 除人工噪声的原因外, 用户对数增加也使用户间的干扰增加, 反而使窃听者的窃听速率降低.

图 4 是用户对数 $K = 4$ 时, 用户和速率、窃听节点和速率、系统保密和速率随源节点发送功率变化的曲

线. 仿真中固定设置中继节点发送总功率 $P_{RT} = NP_R = 0.8\text{W}$, $\beta = 0.2$, 即人工噪声功率 $P_{nr} = 0.2P_R$; 目的节点发送人工噪声功率 $P_{nd} = 0.2\text{W}$. 从仿真结果可知, 当窃听节点没有用户间干扰消除能力时, 保密和速率随 P_s 的增加而增加, 后趋于一个收敛值. 这是因为在源节点发送功率较小时, 源节点发送功率增大, 第 1 跳中继接收信干噪比改善, 相应合法信道的传输速率增加; 而窃听节点由于没有用户间干扰消除的能力, 源节点发送功率增加时用户间干扰也同样增加, 同时还受到人工噪声的干扰, 窃听速率并不能以同样的速度增加, 因此保密速率增加. 而当源节点发送功率增加到一定程度后, 由于中继的发送功率没有增加, 合法信道的传输速

率将受到中继和目的节点间信干噪比的制约, 因此增速降低, 而窃听节点拦截速率的增长与之相当, 因此保密速率不再增加. 当窃听节点具备用户间干扰消除能力时, 保密速率则是随源节点发送功率增加先增加后下降. 这是因为窃听者具有用户间干扰消除能力时, 其第 1 跳中拦截信息的能力将随源节点发送功率的增加而增加, 而合法信道的传输速率还受限于中继和目的节点的信干噪比, 在源节点发送功率增加到一定程度后, 合法信道速率增加速度将低于窃听信道, 保密和速率反而下降. 从中继天线数来看, 中继天线数越大, 阵列增益也越大, 因此系统的保密和速率也越大.

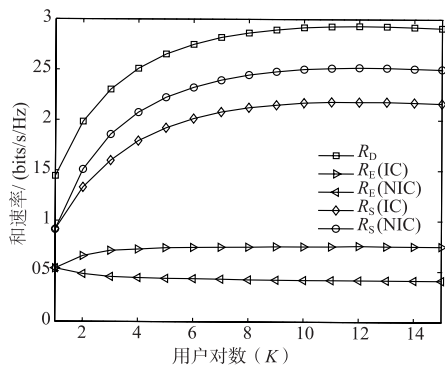


图3 用户对数与系统和速率关系

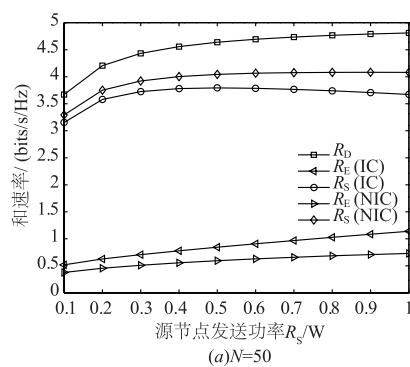


图4 源节点功率与系统和速率的关系

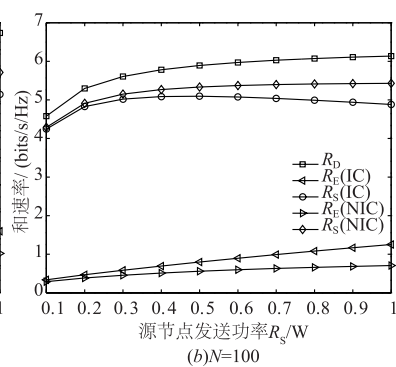


图 5 是用户对数 $K = 4$ 时, 用户和速率、窃听节点和速率、系统保密和速率随目的节点人工噪声功率变化的曲线. 仿真中固定设置中继节点发送总功率 $P_{RT} = NP_R = 0.2\text{W}$, $\beta = 0.2$, 即人工噪声功率 $P_{nr} = 0.2P_R$; 源节点发送功率 $P_s = 0.4\text{W}$. 仿真结果可知, 不管窃听节点是否具备用户间干扰消除能力, 系统保密和速率都是随目的节点人工噪声功率呈现先增长后下降的趋势. 虽然第 1 跳中, 大规模 MIMO 中继接收信号时具有一定的分辨各用户信号的能力, 但目的节点发送的噪声仍然会对其接收源节点信号的信干噪比造成一定的影响. 当 P_{nd} 增大到一定程度时, 其继续增大时使合法信道速率下降的速度高于窃听信道时, 就会引起保密速率下降. 另一方面, 窃听节点具备用户间干扰消除能力的情况下, 目的节点人工噪声功率增加时窃听信道速率的下降速度更快, 此时目的节点发送的人工噪声提高保密速率的效果更为显著.

图 6 是用户对数 $K = 4$, 中继天线数 $N = 100$ 时, 用户和速率、窃听节点和速率、系统保密和速率随中继人工噪声分配比例变化的曲线. 仿真中固定设置源节点发送功率 $P_s = 0.4\text{W}$, 目的节点发送人工噪声功率 $P_{nd} = 0.2\text{W}$. 从仿真结果可知, 当中继节点总功率 P_{RT} 较小时, 中继节点发送人工噪声功率增加反而导致保密速率下降. 这是因为增加人工噪声功率, 相应信号转发功

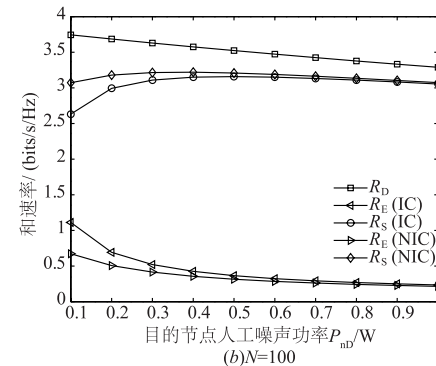
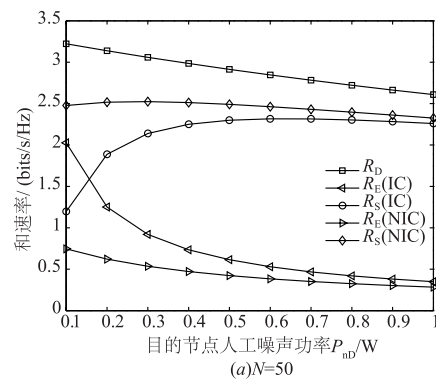


图5 目的节点人工噪声功率与系统和速率关系

率下降, 在中继可用功率较小时, 会导致合法信道速率的明显下降, 而窃听节点可在两跳中都能接收到信号,

窃听信道速率下降速度相对较慢. 而当中继节点总功率 P_{RT} 较大时, 分配适当人工噪声功率则有助于提高保密速率. 这是因为中继链路的传输速率与第 1 跳和第 2 跳的传输性能都有关系, 在源节点的发送功率固定的情况下, 由于受到第 1 跳传输性能的制约, 中继链路的

速率并不会随中继节点转发功率的增加而持续增加. 此时, 如果在中继节点适当分配一些功率用于发送人工噪声, 则可在对合法信道速率影响不大的情况下, 有效降低窃听信道速率, 特别是对窃听者具备多用户干扰消除能力时效果更为显著, 增大保密速率.

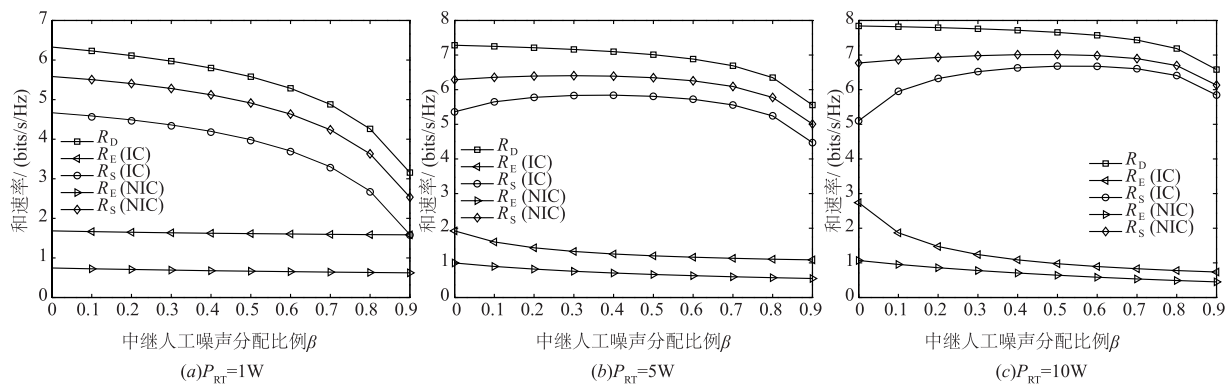


图6 中继人工噪声分配比例与系统和速率关系

图 7 是用户数 $K=4$ 时, 保密能量效率随目的节点人工噪声功率变化的曲线. 仿真中继天线数 $N=50$ 和 100; 固定设置源节点发送功率 $P_s=0.01W$; 中继节点发送总功率 $P_{RT}=NP_R=0.03W$, $\beta=0.3$, 即人工噪声功率 $P_{nr}=0.3P_R$. 从仿真结果显示, 系统保密能量效率随着目的节点人工噪声功率的增加呈现先增长后下降的趋势. 尽管目的节点发送的人工噪声对合法接收者接收速率的提高没有任何帮助, 但是能有效地抑制窃听者的接收质量, 显著降低其窃听速率, 从而提高保密速率. 人工噪声的使用对于窃听节点不能消除用户间干扰时的保密能量效率的提高更为有效. 但当人工噪声功率过大时, 则会引起保密能量效率的下降. 因此, 目的端应用适当的功率发送人工噪声, 可提高系统的保密能量效率.

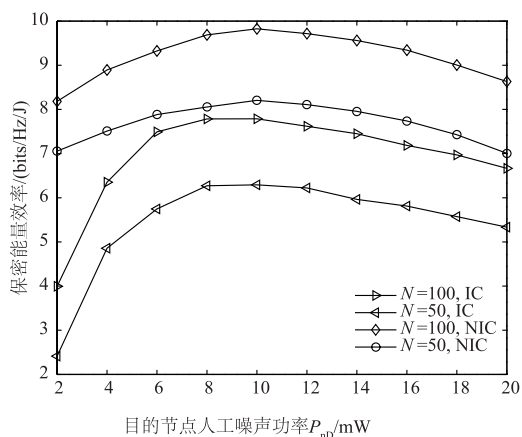


图7 目的节点人工噪声与系统保密能量效率关系

图 8 是用户数 $K=4$ 时, 保密能量效率随中继人工噪声分配比例变化的曲线. 仿真中继天线数 $N=50$

和 100; 固定设置源节点发送功率 $P_s=0.01W$; 目的节点发送人工噪声功率 $P_{nd}=0.01W$; 中继节点发送总功率 $P_{RT}=NP_R=0.04W$. 从仿真结果可知, 与目的端人工噪声对保密能量效率的影响类似, 虽然中继分配部分功率用于发送人工噪声, 会降低合法接收端的接收性能, 但更能有效地恶化窃听者的接收性能, 特别是在窃听者具有多用户间干扰消除的能力时, 人工噪声的效果更为明显. 但人工噪声分配比例过大则会导致保密能量效率下降, 因此适当分配中继的部分功率用于发送人工噪声有利于保密能量效率的改善.

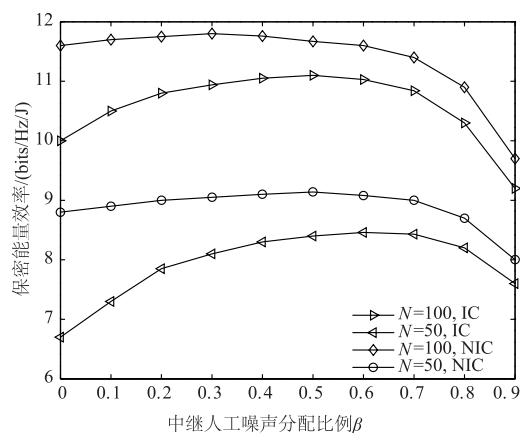


图8 中继人工噪声分配比例与系统保密能量效率关系

图 9 是文献[15]、文献[12]的物理层方案与本文方案性能对比的仿真结果, 与本文类似, 这两个方案中也是采用大规模 MIMO 中继节点进行多个用户对信息的转发. 文献[15]中大规模 MIMO 节点采用迫零准则处理收发信号, 并采用复高斯随机矩阵的伪逆作为人工噪声波束赋形矩阵, 复杂度低于常规的零空间人工

噪声方案. 文献[12]中大规模 MIMO 节点则与本文类似, 采用零空间人工噪声方案. 两种方案都没有针对窃听器可能获得源节点的发送信号设计保护措施. 仿真中, 固定用户对数 $K=4$, 并保持所有方案的发送总功率相同. 图 9(a) 是系统保密和速率随中继天线数变化的仿真结果, 图 9(b) 是系统保密能量效率与中继人工噪声分配比例的关系的仿真结果, 仿真中, 本文方案源节点发送功率为 0.2W, 中继节点发送总功率为 0.2W, 目的节点发送人工噪声功率为 0.2W; 两种对比方案中目的节点不发生人工噪声, 因此我们将两对比方案中的源节点和中继节点发送功率分别增加至 0.3W 和 0.6W, 以保持发送总功率与本文方案相同. 图 9(a) 中的中继人工噪声分配比例 $\beta=0.4$, 图 9(b) 中中继天线数 $N=100$. 仿真结果显示, 本文方案针对第一跳时窃听器可能窃取到源节点发送的信息, 由目的用户发送人工噪声对窃听器进行干扰, 对于提高安全传输性能具有很好的效果, 因而可获得更大的保密速率. 而文献

[15] 方案的性能最差, 主要原因在于其采用的人工噪声波束赋形矩阵为随机产生, 不能使人工噪声位于合法信道的零空间中, 对合法用户的接收造成干扰, 但其实现复杂度较低. 另外本文和文献[12]的方案采用的最大比合并/传输预编码的复杂度较[15]方案的迫零算法低, 但仍然有较好的效果. 图 9(c) 则是系统保密能量效率随目的节点人工噪声功率的变化仿真结果, 仿真中, 中继天线数 $N=100$, 中继人工噪声分配比例 $\beta=0.4$, 中继节点发送总功率为 0.2W; 本文方案中, 在保持源节点与目的节点功率之和固定为 0.4W 的条件下, 目的节点的人工噪声功率从 0W 增加至 0.3W; 两种对比方案的源节点发送功率固定为 0.4W. 两个对比方案中目的节点不发送人工噪声, 故其性能不变. 可以看到, 尽管人工噪声的使用降低了保密信号的发送功率, 但人工噪声能有效地保护保密信号, 因此使用适当功率的人工噪声反而能提高系统保密能量效率, 图 9(b)、(c) 的仿真结果表明了这一点.

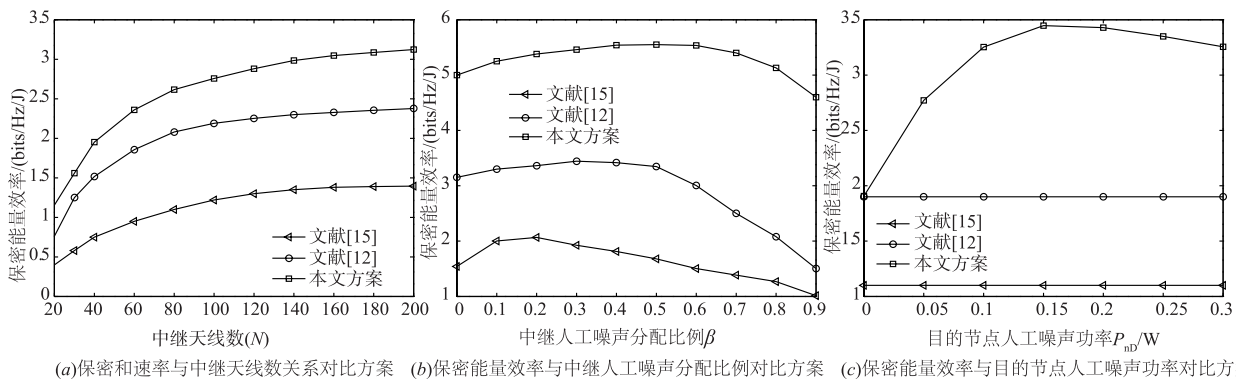


图9 关于本文方案与对比方案仿真

5 总结

本文研究了基于大规模 MIMO 中继的多用户物理层安全传输技术, 系统模型中多个源节点与目的节点通过中继同时通信, 存在被动的窃听节点, 能窃听到源节点和中继发送的信号. 在合法节点不能获得窃听信道的状态信息的情况下, 采用中继 MRC/MRT 信号波束赋形与合法信道零空间人工噪声方案, 并由目的节点在第 1 跳中发送人工噪声进行协作干扰. 在窃听节点具有和没有用户间干扰消除能力两种情况下系统的保密性能进行分析, 得到了中继天线数量有限的保密速率, 以及在中继发送总功率固定时, 中继天线数量无限增长时的渐近保密速率. 对所提方案进行仿真, 仿真结果证明渐近保密速率的理论分析结果准确. 仿真结果表明, 采用大规模 MIMO 中继可同时为多对用户提供服务, 通过采用简单的波束赋形方案, 并配合中继零空间人工噪声和目的节点的协作干扰, 在分配适

当的人工噪声功率下, 可获得可观的保密速率, 并能改善保密能量效率.

参考文献

- [1] Shiu Y S, Chang S Y, Wu H C, et al. Physical layer security in wireless networks: a tutorial [J]. IEEE Wireless Communications, 2011, 18(2): 66-74.
- [2] Ma H, Ma P. Beamforming design of decode-and-forward cooperation for improving wireless physical layer security [A]. Proceedings of the IEEE International Conference on Advanced Communications Technology (ICACT) [C]. PyeongChang: IEEE Press, 2012. 41-49.
- [3] Zhang H, Huang Y, Li C, et al. Secure beamforming design for SWIPT in MISO broadcast channel with confidential messages and external eavesdroppers [J]. IEEE Transactions on Wireless Communications, 2016, 15(11): 7807-7819.
- [4] Li Q, Ma W K. Optimal and robust transmit designs for

- MISO channel secrecy by semidefinite programming [J]. IEEE Transactions on Signal Process, 2011, 59(8): 3799 – 3812.
- [5] Chae S H, Wan C, Lee J H, et al. Enhanced secrecy in stochastic wireless networks; artificial noise with secrecy protected zone [J]. IEEE Transactions on Information Forensics & Security, 2014, 9(10): 1617 – 1628.
- [6] 康小磊, 季新生, 黄开枝, 等. 基于信号对齐的动态人工噪声方法 [J]. 电子学报, 2016, 44(11): 2767 – 2772.
Kang Xiao-lei, Ji Xin-sheng, Huang Kai-zhi, et al. A dynamic artificial noise signal alignment based to enhance security [J]. Acta Electronica Sinica, 2016, 44(11): 2767 – 2772. (in Chinese)
- [7] Marzetta T L. Noncooperative cellular wireless with unlimited numbers of base station antennas [J]. IEEE Transactions on Wireless Communications, 2010, 9(11): 3590 – 3600.
- [8] Ngo H Q, Larsson E G, Marzetta T L. Energy and spectral efficiency of very large multiuser MIMO systems [J]. IEEE Transactions on Communications, 2011, 61(4): 1436 – 1449.
- [9] Zhu J, Schober R, Bhargava V K. Secure transmission in multi-cell massive MIMO systems [J]. IEEE Transactions on Wireless Communications, 2014, 13(9): 1286 – 1291.
- [10] Rawat D B, Neupane K, Song M. A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirements [A]. Proceedings of the IEEE Conference on Computer Communications Workshops [C]. San Francisco: IEEE Press, 2016. 53 – 58.
- [11] Wang Y, Baofeng J I, Huang Y, et al. Analysis over spectral efficiency and power scaling in massive MIMO dual-hop systems with multi-pair users [J]. IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2016, 99(9): 1665 – 1673.
- [12] Chen X, Lei L, Zhang H, et al. Large-scale MIMO relaying techniques for physical layer security; AF or DF? [J]. IEEE Transactions on Wireless Communications, 2015, 14(9): 5135 – 5145
- [13] Guo K, Zhang C, Guo Y, et al. Massive MIMO aided secure multi-pair relaying with power control [A]. Proceedings of the IEEE Vehicular Technology Conference (VTC) [C]. Nanjing: IEEE Press, 2016. 1 – 5.
- [14] Cramér, H. Random Variables and Probability Distributions [M]. 3rd ed. UK: Cambridge University Press, 1970.
- [15] Amarasuriya G, Schaefer R F, Poor H V. Secure communication in massive MIMO relay networks [A]. Proceedings of the IEEE International Workshop on Signal Processing [C]. Texas: IEEE Press, 2016. 1 – 5.

作者简介



雷维嘉 男, 1969 年出生, 云南元谋人, 教授、博士, 现主要从事无线和移动通信技术的研究。

E-mail: leiwj@cqupt.edu.cn



王娟兵 女, 1993 年出生, 甘肃白银人, 硕士研究生, 现主要从事无线通信研究。

E-mail: m15340521572_3@163.com