doi:10.11959/j.issn.1000-436x.2017132

基于中继间干扰消除的轮流转发系统安全传输方案

邹羿，黄开枝，康小磊
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对轮流转发系统中非信任中继窃听的问题，提出一种基于中继间干扰消除的安全传输方案。首先，利用可信中继与非信任中继交替转发产生的中继间干扰，恶化非信任中继的窃听条件。然后，利用信号在时域上的相关性进行干扰迭代消除，完全消除合法用户处中继间干扰，提升合法用户接收信号质量。在此基础上，提出了以最小化窃听和容量为目标的快速功率分配算法。分析和仿真结果表明，方案在保障通信效率的同时抑制了非信任中继的窃听，在仿真条件下，系统的保密速率提升了至少 2 bit·s^{-1}·Hz^{-1}。
关键词：轮流转发；非信任中继；中继间干扰；保密速率
中图分类号：TN911.7 **文献标识码**：A

Successive relaying secure transmission scheme based on inter-relay interference cancellation

ZOU Yi, HUANG Kai-zhi, KANG Xiao-lei
(China National Digital Switching System Engineering & Technological R&D, Zhengzhou 450002, China)

Abstract: A secure scheme based on inter-relay interference cancellation was proposed to solve untrusted relay eavesdropping problem in successive relaying systems. First inter-relay interference between trusted relay and untrusted relay was exploited as artificial noise to degrade untrusted relay's eavesdropping condition, then interference iterative cancellation was adapted to improve signal quality at legitimate user by making use of correlation between signals in time domain. Based on this, a quick power allocation algorithm aiming to minimize untrusted relay's sum rate was proposed. Analysis and simulation results show that the proposed scheme suppress untrusted relay's eavesdropping without loss of communication efficiency, a promotion of at least 2 bit·s^{-1}·Hz^{-1} in secrecy rate can be observed.
Key words: successive relaying, untrusted relay, inter-relay interference, secrecy rate

1 引言

全双工(FD, full-duplex)技术能够实现同时收发信号，有效提高了通信速率，是对抗信道衰落的有效手段。但是 FD 中继系统中存在严重的自干扰，如果处理不当会导致系统性能下降[1]，并且硬件成本过高。近年来，有学者提出了轮流转发(SR, successive relaying)技术[2~7]来克服节点半双工(HD, half-duplex)的限制，提高频谱效率，通过利用多个 HD 中继节点轮流协传以模拟 FD 节点，能够实现收发节点之间的连续通信。与 FD 系统类似，SR 系统中存在的中继间干扰(IRI, inter-relay interference)影响了频谱效率的提升，因此，目前的研究主要集中于 IRI 消除技术[3~7]，进一步提高系统效率、吞吐率和分集增益等。

近年来，无线通信系统的安全问题越来越受到人们的重视。一方面，由于无线信道的开放特性，所有的无线通信系统都存在着被窃听的隐患；另一方面，中继协作系统利用节点转发时需要考虑非信任中继(UR, untrusted relay)的安全问题，即

收稿日期：2016-11-04；**修回日期**：2017-04-12
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2014AA01A701）；国家自然科学基金资助项目（No.61379006, No.61521003, No.61701538）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2014AA01A701), The National Natural Science Foundation of China (No.61379006, No.61521003, No.61701538)

UR 可能在转发时被窃听。物理层安全技术利用无线信道的多样性、时变性、互易性和唯一性，是解决无线通信系统中窃听问题的有效方法，该技术成为近年来的研究热点。针对非信任中继的物理层安全问题，目前，取得了一定的研究成果。文献[8]证明使用非信任中继能够提高中继系统的保密速率。文献[9]推导了非信任中继系统的平均保密容量下界。为了提高非信任中继系统的安全性，文献[10]和文献[11]分别研究了单向和双向非信任多天线中继系统中的联合波束成形问题。当源节点与目的节点之间的直达链路存在时，文献[12]提出直达链路与中继链路切换的方案并推导得到保密中断概率的下界。文献[13]提出目的节点发送人工干扰的方案，文献[14]分析其可达分集阶数为 1。针对 SR 系统中存在非信任中继问题的研究还处于发展阶段，文献[15]首次考虑了 SR 系统中存在多个 UR 时的中继选择问题，提出多个中继选择方案并推导了不同方案的保密中断概率和保密分集阶数。然而，目前还未有研究考虑 SR 系统中存在 UR 时的物理层安全传输方案。

针对上述问题，本文设计了一种基于 IRI 消除与波束成形（BFIC, beamforming and IRI cancellation）的安全传输方案。BFIC 方案利用可信中继与 UR 轮流转发产生的 IRI，来降低 UR 的信道质量，另外，通过波束成形设计以及利用合法接收节点接收信号之间的相关性，在合法节点处进行 IRI 迭代消除，提高可信中继链路和合法接收方的信道容量，达到提高目的节点的信干噪比(SINR, signal to interference plus noise ratio)的目的。此外，为了进一步优化性能，本文还提出一种以最小化窃听和容量为目标的快速功率分配算法。仿真结果表明，本文方案利用 UR 高效传输的同时使 SR 系统的保密速率获得了至少 2 $\text{bit}\cdot\text{s}^{-1}\cdot\text{Hz}^{-1}$ 的增益。本文方案提高安全性能的机理如下：1) 通过引入额外的功率，利用信道之间的信道状态信息设计 Alice 波束成形消除可信中继处的 IRI 干扰，提高了主信道容量；2) Bob 利用接收信号之间的相关性对非信任中继转发信号中的IRI进行消除，提高了主信道容量；3) 利用功率分配算法保持了 IRI 对非信任中继的影响，降低了窃听信道容量。通过上述方法增大了主信道容量与窃听信道容量之间的差距，从而有效提升轮流转发系统的安全性能。

2 系统模型

考虑如图 1 所示的 SR 系统，假设源节点(Alice)与合法目的节点(Bob)之间不存在直达径，通过 2 个中继节点的轮流转发实现下行传输。其中，可信中继 R 表示系统内或具有与 Bob 相同安全等级的节点，非信任中继 R_{U} 表示安全等级较低或存在窃听可能的节点。R_{U} 采用 AF 协议，R 采用 DF 协议。假设除了 Alice 配置 N 根天线，其他各节点均为单天线（该场景可以表示多天线基站通过单天线的中间节点与单天线手机用户进行通信），并且每个节点都工作在 HD 模式。从 Alice 到 R_{U}、R 的信道矢量分别定义为 $\boldsymbol{h}_{a,u}\in\mathbb{C}^{1\times N}$、$\boldsymbol{h}_{a,r}\in\mathbb{C}^{1\times N}$。$R_{\text{U}}$、$R$ 到 Bob 之间的信道矢量分别定义为 $\boldsymbol{h}_{u,b}$、$\boldsymbol{h}_{r,b}$，R_{U} 和 R 之间的信道表示为 $\boldsymbol{h}_{u,r}$。假设完美同步并且信道之间具有互易性（即 $\boldsymbol{h}_{i,j}=\boldsymbol{h}_{j,i}^{*}$）。各个节点之间的信道经历平坦慢衰落，服从块（block）瑞利分布，相干时间包含足够多的时隙，时隙数对系统安全性能的影响可忽略。n_i、n_j 表示加性高斯白噪声（AWGN），分别服从 $\mathcal{CN}(0,\sigma^2)$、$\mathcal{CN}(0,\boldsymbol{I}_j\sigma^2)$，其中，$\sigma^2$ 表示噪声的功率。

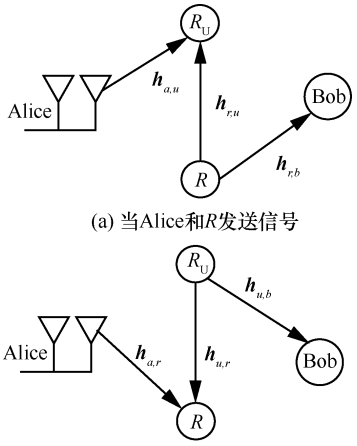


图 1 “轮流中继”通信过程示意

假设需要发送的保密信息平均功率 $\text{E}[\boldsymbol{x}^2]=1$，其中，$\boldsymbol{x}=[x_1\ \ x_2\ \ \cdots\ \ x_M]\in\mathbb{C}^{1\times M}, M\gg 1$。第 k 个保密信息符号由 R_{U} 转发，则该信息表示为 $x_u(k)$，由 R 转发的信息表示为 $x_r(k)$。轮流中继传输开始时，首先由 Alice 向 R_{U} 发送信号 $x_u(1)$，然后 2 个中继节点交替接收、转发来自 Alice 的保密信息。

不失一般性，假设 k 时刻 Alice 以功率为 P_a 向 R_{U} 发送消息 $x_u(k)$，$\boldsymbol{W}_u \in \mathbb{C}^{N\times 1}$ 表示 Alice 在向 R_{U} 发信息时采用的波束成形系数，在本文中所有波束成形系数的范数均为 1，即 $\|\boldsymbol{W}\|=1$。R 以功率 P_r 转发信息 $x_r'(k-1)$, $x_r'(k-1)$ 表示上一时刻 R 接收信号后译码的结果，假设译码正确，则 $x_r'(k-1)=x_r(k-1)$。此时 R_{U} 和 Bob 的接收信号可以表示为

$$y_u(k)=\sqrt{P_a}\boldsymbol{h}_{a,u}\boldsymbol{W}_u x_u(k)+\boldsymbol{h}_{r,u}\sqrt{P_r}x_r(k-1)+n_u(k) \quad (1)$$

$$y_b(k)=\boldsymbol{h}_{r,b}\sqrt{P_r}x_r(k-1)+n_b(k) \quad (2)$$

在 $k+1$ 时刻，R_{U} 以放大系数 w 放大 k 时刻接收的信息 $y_u(k)$，并转发给 Bob，该消息可以表示为

$$x_u'(k)=wy_u(k) \quad (3)$$

其中，放大系数 $w^2=\dfrac{P_r}{P_a\left|\boldsymbol{h}_{a,u}W_u\right|^2}$，使 R_{U} 发射固定功率 P_r 的信号 $x_u(k)$。同时，Alice 向 R 发送 $x_r(k+1)$，假设 Alice 以波束形成系数 $\boldsymbol{W}_r \in \mathbb{C}^{N\times 1}$ 和功率 P_a 向 R 发送 $x_r(k+1)$。此时，R 和 Bob 的接收信号可以表示为

$$y_r(k+1)=\sqrt{P_a}\boldsymbol{h}_{a,r}\boldsymbol{W}_r x_r(k+1)+\boldsymbol{h}_{u,r}x_u'(k)+n_r(k+1) \quad (4)$$

$$y_b(k+1)=\boldsymbol{h}_{u,b}x_u'(k)+n_b(k+1) \quad (5)$$

由式(1)和式(5)可知，R_{U} 放大转发来自 Alice 和 R 的信号，假设 R_{U} 的 *SINR* 简单表示为 $\lambda_u=\dfrac{S}{I+N_u}$，其中，$S$、$I$ 和 N_u 分别表示信号、IRI 和热噪声的功率，经过放大和信道衰落后到达 Bob 时的增益为 G，在 Bob 处信号 SINR 可以表示为 $\lambda_b=\dfrac{GS}{G(I+N_u)+N_b}<\lambda_u$。如果不对 IRI 进行处理，显然该链路上的主信道容量 C_d 小于窃听信道容量 C_e。根据保密速率 C_s 的定义

$$C_s=\left[C_d-C_e\right]^+ \quad (6)$$

其中，$[f]^+=\max(f,0)$，SR 系统在利用 R_{U} 转发时，会出现 C_s 为 0 的问题。

为了提高图 1 所示 SR 系统的保密速率，本文提出了 BFIC 方案，利用 SR 系统中存在的 IRI 代替“人工噪声”来干扰 R_{U}，引入波束成形和干扰迭代消除技术来抵消 IRI 对合法节点的影响，同时保持 IRI 对 R_{U} 信号接收的干扰。

3　BFIC 方案

BFIC 方案通过对合法节点处的 IRI 消除，使 IRI 只对 R_{U} 造成干扰，起到了“人工噪声”的作用，在保持 C_e 不变的同时提高了 C_d，从而使 SR 系统获得非负的 C_s。BFIC 方案分为 2 个部分：Alice 处波束成形和干扰迭代消除。Alice 处波束成形：Alice 在向 R 发送 $x_r(k+1)$ 的同时发送 $x_u(k)$，消除 R 处 $x_u(k)$ 干扰部分。干扰迭代消除：R 的接收信号中包含之前接收时隙的自干扰，Bob 接收来自 R_{U} 转发的信号中包含前一时隙已译码的信息，这些干扰均可以被迭代消除。具体方案如下。

3.1　Alice 处波束成形

首先，考虑在 Alice 处通过对 $x_u(k)$ 的波束成形设计达到消除 IRI 效果。假设 Alice 以波束形成系数 $\boldsymbol{W}_r' \in \mathbb{C}^{N\times 1}$ 和功率 αP_a 向 R 发送保密信息 $x_r(k)$，其中，α 表示用于抵消 R_{U} 干扰的功率分配系数，同时以波束成形系数 $\boldsymbol{W}_r \in \mathbb{C}^{N\times 1}$ 和功率 P_a 向 R 发送保密信息 $x_r(k+1)$。此时，Bob 的接收信号仍如式(5)所示，而 R 的接收信号变为

$$y_r(k+1)=\sqrt{P_a}\boldsymbol{h}_{a,r}\boldsymbol{W}_r x_r(k+1)+I_u+I_r+N \quad (7)$$

其中，$I_u=\sqrt{\alpha P_a}\boldsymbol{h}_{a,r}\boldsymbol{W}_r'x_u(k)+wh_{u,r}\sqrt{P_a}h_{a,u}\boldsymbol{W}_u x_u(k)$、$I_r=w\left|\boldsymbol{h}_{r,u}\right|^2\sqrt{P_r}x_r(k-1)$、$N=w\boldsymbol{h}_{u,r}n_u(k)+n_r(k+1)$。由式(7)可知，$R$ 的接收信号可以分为 4 个部分：有用信号部分 $\sqrt{P_a}\boldsymbol{h}_{a,r}\boldsymbol{W}_r x_r(k+1)$、中继间干扰部分 I_u、自信号干扰部分 I_r 和热噪声部分 N。

为提高 R 的接收信号质量，消除 IRI 对接收信号质量的影响，本文在 Alice 处进行波束成形设计，目的是消除式(7)中干扰 I_u。首先，为了最大化有用信号功率，对于保密信息 $x_r(k+1)$，Alice 采用最大比波束成形传输，可得 $\boldsymbol{W}_r=\dfrac{\boldsymbol{h}_{a,r}^{\mathrm{H}}}{\left\|\boldsymbol{h}_{a,r}\right\|}$；然后，考虑 $\boldsymbol{W}_r'$、$\boldsymbol{W}_u$ 的联合设计使中继间干扰部分叠加后为 0，即 $I_u=0$。$\boldsymbol{W}_u$ 是 Alice 在向 R_{U} 发送信号时采用的波束成形系数，由式(6)可知，为了让 Bob 在接收信号 $x_u(k)$ 时获得尽量大的功率，采用最大比传输波束成形，令

$$\boldsymbol{W}_u=\frac{\left(\boldsymbol{h}_{u,b}\boldsymbol{h}_{a,u}\right)^{\mathrm{H}}}{\left\|\boldsymbol{h}_{u,b}\boldsymbol{h}_{a,u}\right\|}=\frac{\boldsymbol{h}_{a,u}^{\mathrm{H}}\boldsymbol{h}_{u,b}^{\mathrm{H}}}{\left\|\boldsymbol{h}_{u,b}\boldsymbol{h}_{a,u}\right\|} \tag{8}$$

将式(8)代入 $w^2=\dfrac{P_r}{P_a\left|\boldsymbol{h}_{a,u}\boldsymbol{W}_u\right|^2}$ 可得 $w^2=\dfrac{P_r}{P_a\left\|\boldsymbol{h}_{a,u}\right\|^2}$，再将 $\boldsymbol{W}_u$ 和 w^2 代入 $I_u=0$ 中求解 $\boldsymbol{W}_r'$，可得

$$\boldsymbol{W}_r'=-\frac{\boldsymbol{h}_{a,r}^{\mathrm{H}}\boldsymbol{h}_{u,r}\boldsymbol{h}_{u,b}^{\mathrm{H}}}{\sqrt{\alpha\rho}\left|\boldsymbol{h}_{u,b}\right|\left\|\boldsymbol{h}_{a,r}\right\|^2} \tag{9}$$

其中，功率分配系数 $\rho=\dfrac{P_a}{P_r}$，考虑到 Alice 在基站端功率可调节范围较大，因此，本文固定 R 的发射功率为 P_r；根据 $\left\|\boldsymbol{W}_r'\right\|=1$ 可解得

$$\alpha=\frac{\left|\boldsymbol{h}_{u,r}\right|^2}{\rho\left\|\boldsymbol{h}_{a,r}\right\|^2} \tag{10}$$

由式(10)可以得 α 是 ρ 的函数，确定了 ρ 就能确定 α 和 $\boldsymbol{W}_r'$。

3.2 干扰迭代消除

本文提出 IRI 迭代消除的方法消除 R 以及 Bob 接收信号中历史接收信号的干扰。IRI 迭代消除是指节点在每次接收信号时利用已知的信息和节点之间共享的 CSI，将接收信号中的已知信息干扰部分精确消除，该方法有效解决了 IRI 在目的节点累积的问题。

首先是 R 处的干扰迭代消除。假设 R 已经成功译码 $x_r(k-1)$，同时，R 可以获得节点之间的 CSI，因此，R 能够计算得到 $I_r=w\left|\boldsymbol{h}_{r,u}\right|^2\sqrt{P_r}x_r(k-1)$，从而消除自信号干扰部分 I_r。经过上述信号处理过程后，R 的接收信号可变为

$$y_r'(k+1)=\sqrt{P_a}\boldsymbol{h}_{a,r}\boldsymbol{W}_r x_r(k+1)+w\boldsymbol{h}_{u,r}n_u(k)+n_r(k+1) \tag{11}$$

为了提高 Bob 处接收信号的 *SINR*，同样在 Bob 处采用 IRI 迭代消除。由式(5)可知，假设 Bob 在 k 时刻已经成功译码 $x_r(k-1)$，在 $k+1$ 时刻对信息 $x_u(k)$ 译码时，可消除接收信号中的干扰项 $w\boldsymbol{h}_{u,b}\boldsymbol{h}_{r,u}\sqrt{P_r}x_r(k-1)$，此时，Bob 的接收信号可以表示为

$$y_b'(k+1)=w\sqrt{P_a}\boldsymbol{h}_{u,b}\boldsymbol{h}_{a,u}\boldsymbol{W}_u x_u(k)+w\boldsymbol{h}_{u,b}n_u(k)+n_b(k+1) \tag{12}$$

上述方法对于 R_{U} 的接收信号均无影响，由式(1)可得，在 P_r 固定的情况下，可通过 P_a 即 ρ 的设置来改变 R_{U} 的信道容量，本文将在第 4 节从安全的角度讨论 ρ 的设置问题。

综上所述，BFIC 方案实施步骤如下所示。

Step1 CSI 获取阶段，Alice 根据各节点之间的 CSI 计算得到 α、P_a、$\boldsymbol{W}_u$、$\boldsymbol{W}_r$ 与 $\boldsymbol{W}_r'$。

Step2 $k=1$ 时，Alice 以 $\boldsymbol{W}_u$ 发送信息 $x_u(1)$，R_U 接收信号 $y_u(1)$。

Step3 $k\geqslant 2$ 且 k 为偶数时，Alice 发送 $\sqrt{P_a}\boldsymbol{W}_r x_r(k)+\sqrt{\alpha P_a}\boldsymbol{W}_r' x_u(k-1)$，$R_{\mathrm{U}}$ 放大转发 $y_u(k-1)$，R 接收信号 $y_r(k)$ 后减去 $w\left|h_{r,u}\right|^2\sqrt{P_r}x_r(k-2)$ 得到 $y_r(k)$，Bob 接收信号 $y_b(k)$ 后减去 $w\boldsymbol{h}_{u,b}\boldsymbol{h}_{r,u}\sqrt{P_r}x_r(k-2)$ 得到 $y_b'(k)$ 并译码 $x_u(k-1)$。

Step4 $k\geqslant 3$ 且 k 为奇数时，Alice 以 $\boldsymbol{W}_u$ 发送信息 $x_u(k)$，R 译码转发 $x_r(k-1)$，R_{U} 接收信号 $x_u(k)$，Bob 接收信号 $y_b(k)$ 并译码 $x_r(k-1)$。

Step5 重复 Step3 和 Step4 直至信息发送结束或 CSI 变化。

4 安全性能分析

如图 1 所示，在存在 UR 的 SR 模型中，由于 R_{U} 能接收到相邻 2 个时刻的保密信息，因此，本文中保密速率 C_s 有如下表达形式。

$$C_s=\frac{1}{2}\left((C_{rb}-C_{re})^{+}+[C_{ub}-C_{ue}]^{+}\right) \tag{13}$$

其中，$C_{ue}=\mathrm{lb}(1+\lambda_{ue})$、$C_{re}=\mathrm{lb}(1+\lambda_{re})$ 分别表示 R_{U} 窃听保密信息 $x_u(k)$、$x_r(k)$ 时的信道容量，$C_{ub}=\mathrm{lb}(1+\lambda_{ub})$、$C_{rb}=\mathrm{lb}(1+\lambda_{rb})$ 分别表示 Bob 接收保密信息 $x_u(k)$、$x_r(k)$ 时的信道容量，$\lambda_{rb}=\min\{\lambda_{r1},\lambda_{r2}\}$，这是由于 R 采用 DF 协议，该链路的信道容量取决于两跳中最小的一跳。

由式(1)可以计算得到 R_{U} 的信道容量。

$$\lambda_{ue}=\frac{\rho P_r\left\|\boldsymbol{h}_{a,u}\right\|^2}{P_r\left|\boldsymbol{h}_{r,u}\right|^2+\sigma^2} \tag{14}$$

$$\lambda_{re}=\frac{P_r\left|\boldsymbol{h}_{r,u}\right|^2}{\rho P_r\left\|\boldsymbol{h}_{a,u}\right\|^2+\sigma^2} \tag{15}$$

如果采用 BFIC 方案，由式(2)、式(11)和式(12)，

可以计算得到

$$\lambda_{ub}=\frac{\rho P_r\left|\boldsymbol{h}_{u,b}\right|^2\left\|\boldsymbol{h}_{a,u}\right\|^2}{\left(\left|\boldsymbol{h}_{u,b}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2} \tag{16}$$

$$\lambda_{r1}=\frac{\rho P_r\left\|\boldsymbol{h}_{a,u}\right\|^2}{\left|\boldsymbol{h}_{u,r}\right|^2\sigma^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\sigma^2} \tag{17}$$

$$\lambda_{r2}=\frac{P_r\left|\boldsymbol{h}_{r,b}\right|^2}{\sigma^2} \tag{18}$$

由于 lb 函数是一个单调递增的函数，因此，最大化 C_s 近似等价于最大化 $\frac{(1+\lambda_{ub})(1+\lambda_{rb})}{(1+\lambda_{ue})(1+\lambda_{re})}$。根据式(14)~式(18)可知，$\lambda_{ue}$、$\lambda_{re}$、$\lambda_{ub}$ 和 λ_{rb} 都是功率分配系数 ρ 的函数，因此，最大化 C_s 就是要找到最佳的功率分配系数 ρ^*。但是，由于 C_s 的表达式中存在着 $[f]^+$、$\min\{f,g\}$ 等非线性函数，求解 ρ^* 是一个 NP 问题，因此，本文提出了一种快速求解次优 ρ 取值的方法。该方法从最小化 UR 窃听和速率 $C_{ue}+C_{re}$ 的角度出发，由式(1)可得，$\rho_1=\frac{\left|\boldsymbol{h}_{r,u}\right|^2}{\left\|\boldsymbol{h}_{a,u}\right\|^2}$。

本文提出了一种快速功率分配的算法，从最小化窃听和速率的角度出发，经过化简、推导后得到的功率分配系数为 2 个信道增益相除，相比一维搜索的算法有如下两点优势：1) 降低了计算复杂度；2) 不需要迭代计算，避免了求解带来的时延。

如果不采用 BFIC 方案，波束成形系数均采用 MRT 系数，由式(2)和式(5)可知

$$\lambda'_{ub}=\frac{P_a\left|\boldsymbol{h}_{u,b}\right|^2\left\|\boldsymbol{h}_{a,u}\right\|^2}{P_r\left|\boldsymbol{h}_{u,b}\right|^2\left|\boldsymbol{h}_{r,u}\right|^2+\left(\left|\boldsymbol{h}_{u,b}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2} \tag{19}$$

$$\lambda'_{r1}=\frac{P_a\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\left\|\boldsymbol{h}_{a,r}\right\|^2}{P_a\left|\boldsymbol{h}_{u,r}\right|^2\left\|\boldsymbol{h}_{a,u}\right\|^2+P_r\left|\boldsymbol{h}_{r,u}\right|^4\left\|\boldsymbol{h}_{a,u}\right\|^2+\left(\left|\boldsymbol{h}_{u,r}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2} \tag{20}$$

其中，$\lambda'_{rb}=\mathrm{lb}\left(1+\min\left(\lambda'_{r1},\lambda_{r2}\right)\right)$。

由此可以对比 BFIC 方案在系统保密速率方面的提升，在主信道容量方面，由于信道容量的表达式都具有 $\mathrm{lb}(1+\lambda)$ 的形式，因此，只需要将信噪比 λ 部分相除就能比较两式大小，分别将式(17)与式(20)、式(18)与式(21)相除，运算结果如下

$$\frac{\lambda_{ub}}{\lambda'_{ub}}=\frac{P_r\left|\boldsymbol{h}_{u,b}\right|^2\left|\boldsymbol{h}_{r,u}\right|^2+\left(\left|\boldsymbol{h}_{u,b}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2}{\left(\left|\boldsymbol{h}_{u,b}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2} \tag{21}$$

$$\frac{\lambda_{r1}}{\lambda'_{r1}}=\frac{I+\left(\left|\boldsymbol{h}_{u,r}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2}{\left(\left|\boldsymbol{h}_{u,r}\right|^2+\rho\left\|\boldsymbol{h}_{a,u}\right\|^2\right)\sigma^2} \tag{22}$$

其中，$I=P_a\left|\boldsymbol{h}_{u,r}\right|^2\left\|\boldsymbol{h}_{a,u}\right\|^2+P_r\left|h_{r,u}\right|^4\left\|\boldsymbol{h}_{a,u}\right\|^2$，显而易见，式(21)和式(22)的分母部分均包含分子部分，因此，式(21)、式(22)的计算结果均严格大于 1，即 BFIC 方案有效提升了 C_d。对于 UR 而言，进行轮流中继时引入的 IRI 会导致 C_e 的降低，而 BFIC 方案对 UR 信道质量的影响较小。综上所述，在发射功率保持不变的情况下，BFIC 方案在保持 C_e 不变的同时有效提升了 C_d，使 $C_s=\left[C_d-C_e\right]^+$ 增大，增强了系统的安全性能。

5　仿真实验及性能分析

为了证实 BFIC 方案对提高 SR 系统安全性能的有效性，本文对不采用 BFIC 方案的轮流中继模型（简称 SR）、文献[15]中的 UR 安全轮流中继（SSRUR，secure successive relaying with untrusted relay）方案和采用 BFIC 方案的轮流中继模型进行了仿真。统一设置的仿真参数如下：高斯白噪声的功率为 1，信道衰落因子 $\alpha=-3.5$，蒙特卡洛仿真的次数为 10^5，仿真结果及分析如下。

首先是对称拓扑结构下的仿真情况。图 2 展示了当节点位置固定，中继发射功率 P_r 变化时，BFIC 方案、用一维搜索方法找到 ρ^* 的 BFIC-Optimal (BFIC-Op)方案及其对应相同功率条件下 SR 方案、SSRUR 方案保密速率变化情况，其中，各节点的坐标为 Alice$(0,0)$、$R_{\mathrm{U}}(1,-1)$、$R(1,1)$、Bob$(2,0)$，Alice 天线数为 2。仿真结果如图 2 所示，可以明显看出，当采用 SR 方案时，利用 UR 进行轮流通信的保密速率保持在一个较低的水平，并且不随中继节点发射信噪比的上升而增加；相同功率条件下，本文提出的 BFIC 方案相比 SR 方案保密速率得到有效提升，保密速率的差距分别在 2 bit·s^{-1}·Hz^{-1} 以

上，并且该优势随着中继发射信噪比的提高越来越明显。相比文献[15]的 SSRUR 方案，BFIC 方案对于保密速率的提升更明显，BFIC 中的可信中继给系统带来了一定的安全增益。此外，BFIC 方案与 BFIC-op 方案的保密速率存在大概 1 bit·s^{-1}·Hz^{-1} 的差距。

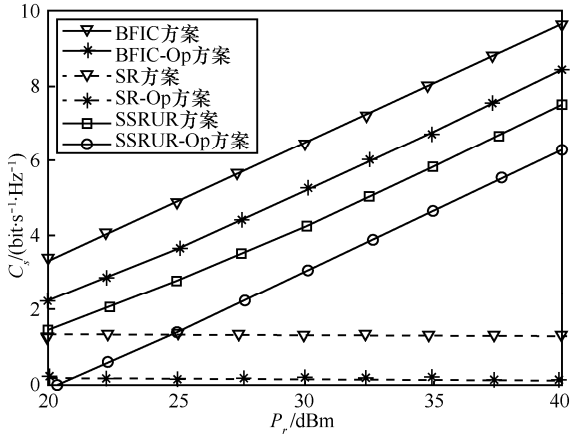


图 2 保密速率随中继发射功率变化

保持上述仿真条件不变，图 3 展示了 BFIC、SR、SSRUR 方案下安全能效（保密速率与消耗的总功率之比）的变化情况。仿真结果表明，随着中继发射信噪比的增加，BFIC 方案的安全能效呈现逐渐降低的趋势，这是因为在信道稳定的情况下中继发射功率的增加会导致 IRI 增大，从而引起用于消除 R 处 IRI 的功率分配系数增大，因而保密速率的增长与总功率的增加不成正比，安全能效逐渐下降。另一方面，BFIC 方案的安全能效最高，SSRUR 方案的安全能耗在不同功率分配下规律不同，表明本文提出的功率分配方案不适用于 SSRUR 方案。

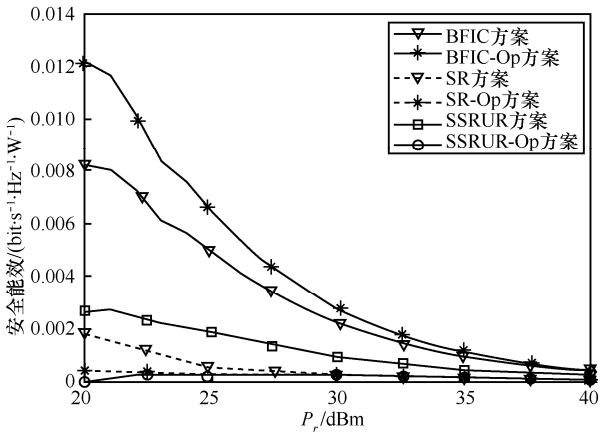


图 3 安全能效随中继发射功率变化

保持其他仿真条件不变，固定中继发射信噪比为 30 dB，图 4 和图 5 分别展示了 R_U 与 R 在横坐标同时变化时（保持关于横坐标对称的位置）保密速率（C_s）和安全能效的变化情况。从图 4 可以看出，随着中继由 Alice 逐渐向 Bob 移动，在固定中继发射功率的情况下 BFIC 方案的保密速率逐渐增加，并且 BFIC 与最优方案的差距逐渐增大。由于本文算法的物理含义是通过调整 Alice 发射功率得 2 条路径的保密信息在非信任中继处强度相同，当中继由 Alice 逐渐向 Bob 移动，中继到 Alice 的距离增大，中继之间的距离并没有变化即中继间干扰的强度不变。此时，为了实现最小化窃听和速率的目标，弥补中继到 Alice 的距离增大带来的信道增益损失，Alice 必须增加发射功率，即在窃听和速率不变、Alice 发射功率增加的情况下，可信中继传输的信息速率提高，因此保密速率逐渐增加。本文方案只考虑了窃听速率，

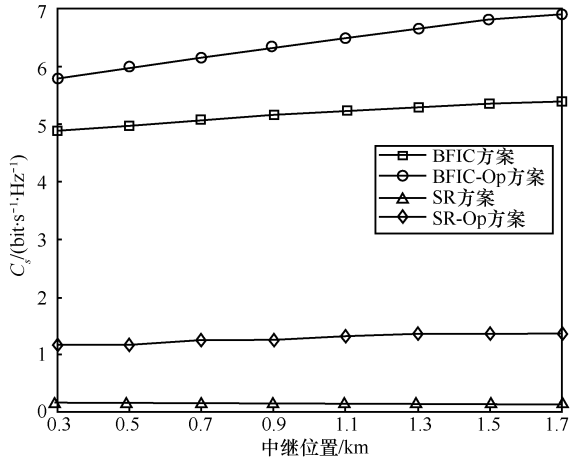


图 4 保密速率随中继位置变化

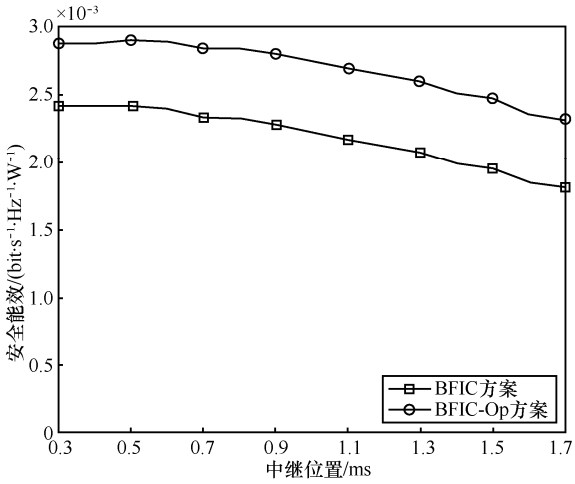


图 5 安全能效随中继位置变化

其目标函数不是保密速率，是次优的功率分配方案，在节点位置固定的情况下其与最优方案存在差距。BFIC 与最优方案的差距逐渐增大的原因就在于最优方案将更多功率用于提升主信道容量方面，相比本文提出的功率分配方案更有效率，因此，在总功率增加时保密速率的差距也在逐渐增加。图 5 展示的安全效率变化规律也与实际符合，即当中继之间的距离不变，随着中继节点远离 Alice，系统的安全效率逐渐降低，这是因为 Alice 用于消除 R 处 IRI 的功率逐渐增大。

保持其他仿真条件不变，固定中继发射信噪比 20 dB，固定 $R_{\mathrm{U}}(1,-1)$ 位置不变，图 6 和图 7 分别展示了 BFIC 和 BFIC-Op 方案下保密速率随 R 位置变化时的仿真结果。如图 6 所示，当采用 BFIC 方案时，保密速率在 R 接近 Bob 时最大，如随着 R 沿着 X 轴向 Bob 移动，保密速率逐渐增大，这是因为本文所提功率分配算法的物理含义是通过调整 Alice 发射功率获得 2 条路径的保密信息在 UR 处强度相同，

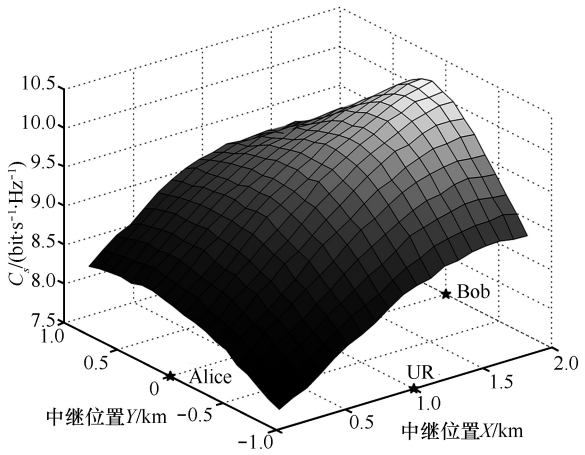


图 6　BFIC 方案保密速率随可信中继位置变化

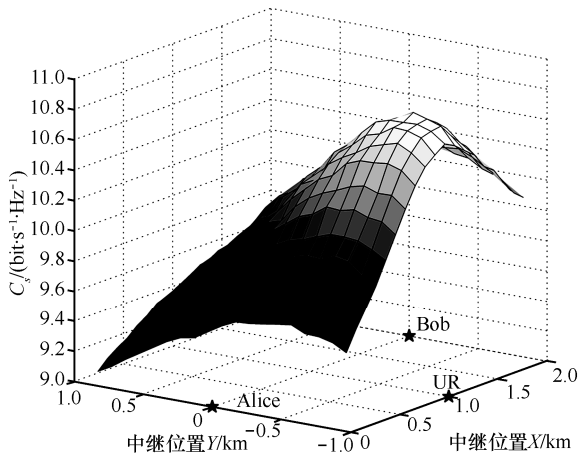


图 7　BFIC-Op 方案保密速率随可信中继位置变化

在中继间距离不变、中继发射功率不变的情况下，Alice 需要增加额外的发射功率来实现干扰消除，主信道容量以及保密速率也随着 Alice 发射功率的增加而提高；而在 Y 轴方向，保密速率呈现先增大后减小的规律，说明 IRI 取某个中间值时最优；图 7 所示规律与图 6 略有不同，当采用 BFIC-Op 方案时，保密速率最大值没有出现在最靠近 Bob 的位置，而是先增大后减小。此外，将图 6 与图 7 的数值进行对比，BFIC 方案始终小于 BFIC-Op 方案。

6　结束语

本文针对轮流转发系统中非信任中继窃听的问题，提出一种基于 IRI 消除的轮流转发安全传输方案。该方案利用可信中继和非信任中继交替转发产生的 IRI 恶化非信任中继的信号接收条件，实现类似“人工噪声”的效果，同时，通过基站端的波束成形设计、中继节点和 Bob 处的干扰迭代消除保证了 Bob 接收信号的质量。分析证实方案的有效性，并提出一种快速功率分配算法。仿真结果表明，本文方案能够提升轮流转发系统的安全性能。未来可针对多个非信任中继存在的场景进行进一步研究。

参考文献：

[1] CHEN G, YU G, PEI X, et al. Physical layer network security in the full-duplex relay system[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(3):574-583.

[2] YANG S, BELFIORE J C. Towards the optimal amplify-and-forward cooperative diversity scheme[J]. IEEE Transactions on Information Theory, 2006, 53(9):3114-3126.

[3] RANKOV B, WITTNEBEN A. Spectral efficient protocols for half-duplex fading relay channels[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(2):379-389.

[4] LUO C, GONG Y, ZHENG F. Full interference cancellation for two-path relay cooperative networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1):343-347.

[5] WICAKSANA H, TING S H, GUAN Y L, et al. Decode-and-forward two-path half-duplex relaying: diversity-multiplexing tradeoff analysis[J]. IEEE Transactions on Communications, 2011, 59(7):1985-1994.

[6] REN C, CHEN J, KUO Y, et al. Differential successive relaying scheme for fast and reliable data delivery in vehicular ad hoc, networks[J]. IET Communications, 2015, 9(8):1088-1095.

[7] NOMIKOS N, CHARALAMBOUS T, KRIKIDIS I, et al. A buffer-aided successive opportunistic relay selection scheme with power adaptation and inter-relay interference cancellation for cooperative diversity systems[J]. IEEE Transactions on Communications, 2014, 63(5): 1623-1634.

[8] HE X, YENER A. Cooperation with an untrusted relay: a secrecy

perspective[J]. IEEE Transactions on Information Theory, 2009, 56(8): 3807-3827.

[9] SUN L, ZHANG T, LI Y, et al. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes[J]. IEEE Transactions on Vehicular Technology, 2012, 61(8):3801-3807.

[10] JEONG C, KIM I M, DONG I K. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system[J]. IEEE Transactions on Signal Processing, 2012, 60(1):310-325.

[11] MO J, TAO M, LIU Y, et al. Secure beamforming for MIMO two-way communications with an untrusted relay[J]. IEEE Transactions on Signal Processing, 2013, 62(9):2185-2199.

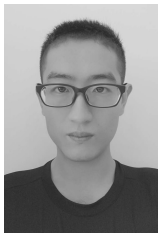
[12] JU M C, KIM D H, HWANG K S. Opportunistic transmission of nonregenerative network with untrusted relay[J]. IEEE Transactions on Vehicular Technology, 2015, 64(6):2703-2709.

[13] HUANG J, MUKHERJEE A, SWINDLEHURST A L. Secure communication via an untrusted non-regenerative relay in fading channels[J]. IEEE Transactions on Signal Processing, 2013, 61(10): 2536-2550.

[14] KIM J B, LIM J, CIOFFI J M. Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays[J]. IEEE Transactions on Wireless Communications, 2015, 14(7): 3866-3876.

[15] WANG W, TEH K C, LI K H. Relay selection for secure successive af relaying networks with untrusted nodes[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(11): 2466-2476.

作者简介：



邹羿（1991-），男，山东济南人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为无线物理层安全、协作通信等。

黄开枝（1973-），女，安徽滁州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为移动通信网络与信息安全等。

康小磊（1986-），男，陕西咸阳人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线物理层安全、D2D通信。