基于有限反馈的非可信中继系统的物理层安全性能分析

吴亚峰[1,2],赵 睿[1,2],贺玉成[1,2],谢维波[1]
(1.华侨大学信息科学与工程学院,福建厦门 361021;
2.西安电子科技大学综合业务网理论及关键技术国家重点实验室,陕西西安 710071)

摘 要: 在基于有限反馈获得部分信道状态信息的条件下,研究了放大转发非可信中继系统的物理层安全传输技术.通过目的节点发送人工噪声干扰信息,使系统获得了正安全容量.推导了安全中断概率和传输中断概率的闭合表达式,分析了反馈比特数对系统安全性和可靠性的影响,进而提出了能同时兼顾系统安全性和可靠性的最优反馈比特数的自适应选择方案.

关键词: 物理层安全;有限反馈;非可信中继;安全中断概率;传输中断概率
中图分类号: TP929.5 **文献标识码:** A **文章编号:** 0372-2112 (2015)11-2247-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.11.017

Performance Analysis of Physical Layer Security of Untrusted Relay System Based on Limited Feedback

WU Ya-feng[1,2], ZHAO Rui[1,2], HE Yu-cheng[1,2], XIE Wei-bo[1]
(1. *School of Information Science and Engineering, Huaqiao University, Xiamen, Fujian* 361021, *China*;
2. *The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Under the condition of partial channel state information that is obtained from limited feedback, a physical layer security transmission technique is investigated for amplify-and-forward untrusted relay systems, where the positive secrecy capacity is obtained through the artificial noise interference information transmitted by the destination node. Closedform expressions for security outage probability and transmission outage probability are derived, and the impacts of the number of feedback bits on security and reliability are analyzed. Furthermore, an adaptive selection scheme for the optimal number of feedback bits is proposed in order to simultaneously satisfy both required security and reliability.

Key words: physical layer security; limited feedback; untrusted relay; security outage probability; transmission outage probability

1 引言

近来,协同中继无线通信系统的安全性问题已受到广泛关注.早期的传统密码体制,直接对信息加密后传输,窃听者和合法接收者都能接收到信号.随着破译算法的日益精进,在某些高安全性要求的环境(例如军事网络)下,传统密码学的方法显得力不从心.物理层安全技术通过充分利用无线信道复杂的空间特性和时变特性,使窃听者无法接收到保密信号,可直接从物理层保障信息传输的安全性.

无线通信物理层安全的核心思想是探究无线通信系统的物理特性以提供安全通信环境.基于香农的信息安全理论,Wyner 首先提出了安全容量概念[1],定义为在窃听干扰下能可靠传输信息的最大速率,反映了可安全传输的信息量的多少,是衡量系统安全性能的标准.最优化的安全通信就是使合法接收节点的容量最大化,同时使窃听节点的容量最小化.

协同中继网络的三节点通信模型与传统搭线(wiretap)通信模型相比,主要区别是前者存在外部窃听节点[1].即使不存在外部窃听,信息也有可能被非可信中

收稿日期:2014-06-19;修回日期:2015-03-09;责任编辑:马兰英
基金项目:国家自然科学基金(No.61401165,No.61271383,No.61201264,No.61302095);泉州市科技计划项目(No.2013Z36);福建省自然科学基金(No.2015J01262,No.2014J01243);华侨大学科研基金(No.13Y0384)

继所窃听.非可信中继在帮助转发信息的同时,也在试图窃听信息,此时非可信中继就成为内部窃听者.例如在政府情报网络以及金融系统网络中,信息经过中继协同网络进行传输时,中继的安全许可等级常常较低,对于待传输信息而言,中继是未授权的.通过引入友好干扰节点,含有非可信中继的协同通信系统可获得正安全容量[2,3].当中继采用解码转发(Decode-and-Forward,DF)方式传输时,中继节点优先于目的节点收到更准确的解码信号,无法获得正安全容量,故非可信中继通信系统一般采用放大转发(Amplify-and-Forward,AF)中继.

当前协同中继系统物理层的安全性能分析主要包括安全容量、安全中断率等[4,5];安全传输方法包括波束成形、协作干扰等[6];安全节点选择方法包括中继选择、友好干扰选择等[7,8].文献[2]针对非可信双向中继系统引入了外部友好干扰节点,推导了安全容量的闭合表达式.文献[3]针对非可信两跳中继系统,推导了关于天线配置、中继转发方式、节点协作策略等不同条件下的安全中断概率.文献[5]针对协作多中继网络,引入外部窃听节点,研究在不同中继转发协议下通过优化安全容量及安全中断概率来进行中继的选择方法.文献[7]针对协同中继窃听网络,提出将一个中继选作友好干扰节点的发送策略,并根据瞬时或平均信道信息做出相应的中继选择.

以上工作均假设发送节点已知完全的信道状态信息(Channel State Information,CSI).然而在许多实际通信场合,发送节点通常难以获得完全 CSI.针对此问题,有限反馈技术可使得发送节点获得部分 CSI.文献[9]针对多输入多输出(Multiple Input Multiple Output,MIMO)系统,提出获得满复用增益条件下反馈比特数的约束条件,并推得量化误差夹角的上下界.文献[10]基于量化信道方向信息以及信道质量信息方法,提出一种低复杂度的半正交用户选择算法,并分析了反馈比特数、用户数量、接收信噪比之间的折中选择.文献[11]针对放大转发中继系统,基于有限反馈和线性波束成形技术推得传输中断概率的闭合表达式.

上述文献仅针对传统 MIMO 信道或中继系统研究了有限反馈对系统容量的影响,并未考虑有限反馈对系统安全传输性能产生的影响.为了解决这个问题,文献[12,13]针对多天线多用户下行链路,研究了获得部分 CSI 情况下有限反馈比特数对遍历安全容量的影响.文献[14]针对 MIMO 网络窃听系统,提出了一种基于有限反馈的预编码方法,研究了安全中断概率关于传输天线数改变的变化趋势.然而,在基于中继的安全传输系统中,有限反馈对系统安全性能的影响未见研究报道.

本文考虑一种较为实际的协同中继网络模型,即部分 CSI 情况下的非可信中继系统,发送节点通过来自中继的有限反馈获得部分 CSI,通过分析系统的传输中断概率和安全中断概率,提出了一种能在可靠性和安全性两方面获得良好折中的有限反馈传输方案.本文针对两跳非可信中继系统,假设发送节点到目的节点不存在直传链路,非可信中继在作为通信的协助者对信号进行放大转发的同时,也作为一个窃听者试图获取发送节点发送的信息.

本文首先给出非可信中继系统模型,引入人工噪声和有限反馈技术;其次推导安全中断概率和传输中断概率的闭合表达式,证明此系统模型下可进行安全通信,且系统的安全性和可靠性均受到反馈比特数的影响;然后研究最优反馈比特数的选择方法;最后,应用仿真方法验证理论分析结果.

本文成果总结如下:

(1) 推导得到引入有限反馈后非可信中继系统的安全中断概率和传输中断概率的闭合表达式.

(2)证明了随着反馈比特数的增加,系统安全性变差,而可靠性则获得提高.

(3)得到同时保证系统安全性和可靠性的最优有限反馈比特数的自适应选择方法.

2 系统模型

图 1 给出了三节点的非可信中继网络系统模型,包括源节点(S),非可信中继节点(R)和目标节点(D).假设 S 和 D 各配有 M 根天线,R 配置单天线,第一时隙经历多输入单输入传输(Multiple Input Single Output,MISO),第二时隙经历单输入多输出传输(Single Input Multiple Output,SIMO).该模型假设源节点到目标节点的距离足够远,因而不考虑 S 到 D 的直传链路,仅使用非可信中继 R 进行放大转发(AF)[7].信道假设为准静态、平坦瑞利衰落信道.每个节点的发送功率均为 P.信道中加性高斯噪声的平均噪声功率为 σ^2.

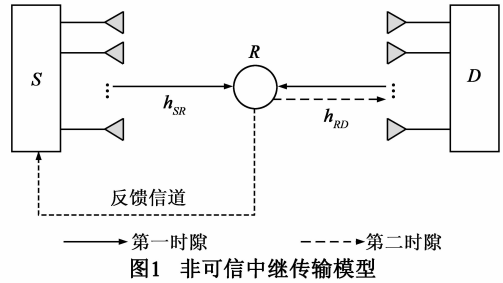

图1 非可信中继传输模型

假设每个节点均已知各信道的完全信道信息 CSI.第一时隙 S 向 R 发送保密信号,最优发送方式为最大比发送(Maximal-Ratio Transmission,MRT)[15],此时 R 的

接收信干噪比(Signal to Interference plus Noise Ratio, SINR)为

$$\gamma_a = \frac{P}{\sigma^2} \| \boldsymbol{h}_{SR} \|^2 \tag{1}$$

第二个时隙 R 向 D 发送信号,并在 D 进行最大比合并(Maximal-Ratio Combining, MRC), D 的接收 SINR 为

$$\gamma_b = \frac{P}{\sigma^2} \frac{\| \boldsymbol{h}_{SR} \|^2 \| \boldsymbol{h}_{RD} \|^2}{\| \boldsymbol{h}_{SR} \|^2 + \| \boldsymbol{h}_{RD} \|^2 + \frac{\sigma^2}{P}} \tag{2}$$

其中 $\boldsymbol{h}_{SR}, \boldsymbol{h}_{RD} \in C^{M\times 1}$ 为零均值复高斯随机向量,分别表示 S-R 和 R-D 的信道系数.

这时,系统安全容量为

$$C' = \frac{1}{2}[\log_2(1+\gamma_b) - \log_2(1+\gamma_a)]^+ \tag{3}$$

其中代$[x]^+$代表 $\max\{x,0\}$.由于第二跳中引入的噪声加大了对原信号的干扰,故中继节点的接收 SINR 必然比目的节点的 SINR 大,使得安全容量等于零,即恒有 $\gamma_a > \gamma_b$,故 $C' = 0$.

本文考虑引入友好干扰而获取正安全容量,实现安全传输.第一时隙 S 向 R 发送待传输信号的同时, D 向 R 发送人工噪声干扰[16].由于 R 事先并不知道接收信号中哪部分是待转发信号,故加入友好干扰信号后将显著降低 R 节点的接收信干噪比 γ_a;而在 D 节点经过对接收信号做自干扰消除,友好干扰不会大幅度降低 γ_b,此时将获取正安全容量.

由于 S 节点常常是一个移动的发送源,如移动用户或移动发送台, S 的物理位置并不固定,故 S 到 R 的信道是时变的,其完全 CSI 较难获得;而 R 和 D 的物理位置相对固定,且由于存在 R 到 D 的传输链路,在发送保密信息之前, D 可通过 R 发送的训练信号估计出 R 到 D 的 CSI,并假设不存在训练估计误差且存在信道互易性,即 $\boldsymbol{h}_{DR} = \boldsymbol{h}_{RD}^H$.因此,本文考虑采用有限反馈技术获取 S-R 信道的 CSI.故 S 节点在正式发送保密信息前首先向 R 发送训练信号, R 在获得 S-R 信道的 CSI 之后,将信道方向信息量化为 B 比特反馈至 S 节点.

令量化码本为 $C^* = \{\boldsymbol{c}_1, \cdots, \boldsymbol{c}_N\}$,其中 $N = 2^B$, B 为反馈比特数.量化码本中每个码字 $\boldsymbol{c}_j$ 是预先随机生成的一个 M 维的复单位向量, M 为 S 节点的天线个数.令 $\boldsymbol{h}_{SR}$的信道方向信息表示为 $\tilde{\boldsymbol{h}}_{SR} = \boldsymbol{h}_{SR} / \| \boldsymbol{h}_{SR} \|$,根据最小弦距离方法[10],得到

$$n = \arg \max_{1\leqslant j\leqslant N} | \tilde{\boldsymbol{h}}_{SR} \boldsymbol{c}_j^* | \tag{4}$$

即 $\tilde{\boldsymbol{h}}_{SR}$估计为 $\hat{\boldsymbol{h}}_{SR} = \boldsymbol{c}_n$.

记 θ 为 $\tilde{\boldsymbol{h}}_{SR}$ 和 $\hat{\boldsymbol{h}}_{SR}$的量化误差夹角,则有 $\cos^2\theta = |\tilde{\boldsymbol{h}}_{SR}^H \hat{\boldsymbol{h}}_{SR}|^2$,且 $\sin^2\theta$ 和 $\cos^2\theta$ 的累积分布函数(Cumulative Distribution Function, CDF)分别为[9,17]

$$F_{\sin^2\theta}(x) = \begin{cases} 2^B x^{M-1}, & 0 \leqslant x \leqslant \delta \\ 1, & x \geqslant \delta \end{cases} \tag{5}$$

$$F_{\cos^2\theta}(x) = \begin{cases} 0, & 0 \leqslant x \leqslant 1-\delta \\ 1 - 2^B (1-x)^{M-1}, & 1-\delta < x < 1 \\ 1, & x > 1 \end{cases} \tag{6}$$

其中 $\delta = 2^{-\frac{B}{M-1}}$.

根据式(5)和式(6)可推得存在紧致上下界:

$$\frac{B}{M-1} \leqslant -E[\log_2 \sin^2\theta] \leqslant \frac{B+\log_2 e}{M-1} \tag{7}$$

S 获得量化信道信息后,第一传输时隙, S 和 D 同时发送信号至 R, R 的接收信号为

$$y_R = \sqrt{P} \boldsymbol{h}_{SR}^H \boldsymbol{w}_{SR} x_1 + \sqrt{P} \boldsymbol{h}_{DR}^H \boldsymbol{w}_{DR} x_2 + n_1 \tag{8}$$

其中, P 为平均发送功率, x_1 为保密信号, x_2 为人工噪声信号, n_1 为零均值复高斯噪声变量. $\boldsymbol{w}_{SR}$和 $\boldsymbol{w}_{DR}$分别为 S 节点和 D 节点的波束成形向量,所以为最大化接收信噪比, S 节点和 D 节点均采用 MRT 方式发送,即 $\boldsymbol{w}_{SR} = \hat{\boldsymbol{h}}_{SR}$, $\boldsymbol{w}_{DR} = \tilde{\boldsymbol{h}}_{DR} = \boldsymbol{h}_{DR} / \| \boldsymbol{h}_{DR} \|$.故式(8)可进一步表示为

$$y_R = \sqrt{P} \boldsymbol{h}_{SR}^H \hat{\boldsymbol{h}}_{SR} x_1 + \sqrt{P} \boldsymbol{h}_{DR}^H \frac{\boldsymbol{h}_{DR}}{\| \boldsymbol{h}_{DR} \|} x_2 + n_1 \tag{9}$$

第一时隙中继节点 R 的接收 SINR 改写为

$$\gamma_1 = \frac{|\tilde{\boldsymbol{h}}_{SR}^H \hat{\boldsymbol{h}}_{SR}|^2 \| \boldsymbol{h}_{SR}^H \|^2}{\| \boldsymbol{h}_{DR}^H \|^2 + \frac{1}{\rho}} \tag{10}$$

其中 $\rho = \frac{P}{\sigma^2}$.

第二时隙, R 向 D 转发信号,中继放大因子为 $1/\| y_R \|$.为最大化接收端信噪比, D 采用 MRC 方式接收,则 D 的接收信号为

$$\begin{aligned} y_D &= \frac{\sqrt{P}}{\| y_R \|} \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{h}_{RD} y_R + \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{n}_2 \\ &= \frac{\sqrt{P}}{\| y_R \|} \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{h}_{RD} \sqrt{P} \boldsymbol{h}_{SR}^H \hat{\boldsymbol{h}}_{SR} x_1 \\ &\quad + \underbrace{\frac{\sqrt{P}}{\| y_R \|} \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{h}_{RD} \sqrt{P} \boldsymbol{h}_{DR}^H \frac{\boldsymbol{h}_{DR}}{\| \boldsymbol{h}_{DR} \|}}_{I_1} x_2 \\ &\quad + \frac{\sqrt{p}}{\| y_R \|} \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{h}_{RD} n_1 + \frac{\boldsymbol{h}_{RD}^H}{\| \boldsymbol{h}_{RD} \|} \boldsymbol{n}_2 \end{aligned} \tag{11}$$

其中 $\boldsymbol{h}_{DR} = \boldsymbol{h}_{RD}^H$, $\boldsymbol{n}_2$ 为零均值复高斯噪声向量. D 节点进行自干扰消除后,将约去 I_1 项[3],接收 SINR 改写为

$$\gamma_2 = \rho \frac{|\tilde{\boldsymbol{h}}_{SR}^H \hat{\boldsymbol{h}}_{SR}|^2 \| \boldsymbol{h}_{SR}^H \|^2 \| \boldsymbol{h}_{DR}^H \|^2}{|\tilde{\boldsymbol{h}}_{SR}^H \hat{\boldsymbol{h}}_{SR}|^2 \| \boldsymbol{h}_{SR}^H \|^2 + 2 \| \boldsymbol{h}_{DR}^H \|^2 + \frac{1}{\rho}} \tag{12}$$

3　性能分析

本节将分析引入有限反馈后的系统安全性和可靠性,分别推导安全中断概率和传输中断概率的闭合表

达式,分析反馈比特数对系统安全性和可靠性的影响.

3.1 安全中断概率

在实际通信场景中,由于 R 到 D 的物理位置相对固定,且存在 R 到 D 的传输链路,故容易获得 *R-D* 信道的 CSI,如上述系统模型中所述.下面的推导中,我们只假设 R 节点已知第一时隙 *R-D* 信道系数的统计平均 $U=E(\|\boldsymbol{h}_{RD}\|^2)$,并完全已知第二时隙 *R-D* 信道系数 $\boldsymbol{h}_{RD}$,令 $G=\|\boldsymbol{h}_{RD}\|^2$.记 $A=\left|\tilde{\boldsymbol{h}}_{SR}^H\hat{\boldsymbol{h}}_{SR}\right|^2$, $C=\|\boldsymbol{h}_{SR}^H\|^2$,则式(10)和式(12)修正为:

$$\tilde{\gamma}_1=\frac{AC}{U+\frac{1}{\rho}} \tag{13}$$

$$\tilde{\gamma}_2=\rho\frac{AGC}{AC+G+U+\frac{1}{\rho}} \tag{14}$$

故安全传输的概率为

$$P\{\tilde{\gamma}_1>\tilde{\gamma}_2\}=P\left\{AC<\rho UG-U-\frac{1}{\rho}\right\} \tag{15}$$

由文献[11]可知,记 $G^*=\rho UG$ 的概率密度函数(Probability Density Function,PDF)为

$$f_{G^*}(x)=\frac{1}{\rho U\Gamma(M)}\left(\frac{x}{\rho U}\right)^{M-1}\mathrm{e}^{-\frac{x}{\rho U}} \tag{16}$$

其中 $\Gamma(\cdot)$为伽马函数,当 x 为正整数时,有 $\Gamma(x)=(x-1)!$

记 $C^*=AC$,即 $C^*=\|\boldsymbol{h}_{SR}^H\|^2\cos^2\theta$,由文献[17]可知 C^* 的 CDF 为

$$F_{C^*}(x)=1-2^B\mathrm{e}^{-x}+\mathrm{e}^{-\frac{x}{1-\delta}}\sum_{k=0}^{M-1}\frac{(\delta^{k-M+1}-1)x^k}{k!(1-\delta)^k} \tag{17}$$

将式(16)和(17)代入式(15),可得

$$P\{\tilde{\gamma}_1>\tilde{\gamma}_2\}=P\left\{C^*<G^*-U-\frac{1}{\rho}\right\} \tag{18}$$

可推得系统安全中断概率(具体推导过程见附录 A)

$$P\{\tilde{\gamma}_1<\tilde{\gamma}_2\}=2^BI_4-I_3 \tag{19}$$

其中

$$I_3=\sum_{k=0}^{M-1}\frac{(\delta^{k-M+1}-1)\mathrm{e}^{-\frac{\rho U+1}{\rho^2U}}}{k!(1-\delta)^k(\rho U)^M\Gamma(M)}\sum_{i=0}^{M-1}\binom{M-1}{i}\cdot\left(U+\frac{1}{\rho}\right)^{M-1-i}\left(\frac{1-\delta+\rho U}{(1-\delta)\rho U}\right)^{k+i+1}\Gamma(k+i+1) \tag{20}$$

$$I_4=\sum_{i=0}^{M-1}\binom{M-1}{i}\left(U+\frac{1}{\rho}\right)^{M-1-i}\left(\frac{\rho U}{1+\rho U}\right)^{i+1}\cdot\frac{\Gamma(i+1)\mathrm{e}^{-\frac{\rho U+1}{\rho^2U}}}{(\rho U)^M\Gamma(M)} \tag{21}$$

类似地,我们亦可推得已知完全 CSI 情况下的非可信中继模型下的安全中断概率如下:

$$P^*\{\gamma_1<\gamma_2\}=\frac{\mathrm{e}^{-\frac{\rho U+1}{\rho^2U}}}{(\rho U)^M\Gamma(M)}\sum_{k=0}^{M-1}\sum_{i=0}^{M-1}\binom{M-1}{i}\cdot\left(U+\frac{1}{\rho}\right)^{M-1-i}\left(\frac{\rho U}{1+\rho U}\right)^{k+i+1}\frac{\Gamma(k+i+1)}{k!} \tag{22}$$

式(19)的 $P\{\tilde{\gamma}_1<\tilde{\gamma}_2\}$是反馈比特数 B 的单调增函数(推导过程见附录 B),即反馈比特数越大,中断概率越大.这是因为随着 B 的增加,会造成 γ_1 增加的幅度比 γ_2 增加的幅度小,即非可信中继 R 与目标节点 D 相比,对发送节点 S 到中继节点 R 的 CSI 准确性更敏感.故可得到结论:反馈比特数越少,安全中断概率越小,系统安全性越好.然而,下一节关于传输中断概率的分析中可知,反馈比特数过小,将会影响系统的可靠性.

3.2 传输中断概率

为了完整地评价系统性能,下面将推导考虑有限反馈条件下的传输中断概率,即接收节点容量未达到目标容量的概率,得到闭合表达式,并分析反馈比特数对系统可靠性的影响.

记 $G_1=\rho AC$, $G_2=\rho G$,其中关于 A、G 和 C 的定义同 3.1 节.由式(16)可知 G_1 的 CDF 为

$$F_{G_1}(x)=1-2^B\mathrm{e}^{-\frac{x}{\rho}}+\mathrm{e}^{-\frac{x}{\rho(1-\delta)}}\sum_{k=0}^{M-1}\frac{(\delta^{k-M+1}-1)x^k}{k!(1-\delta)^k\rho^k} \tag{23}$$

由式(17)可知 G_2 的 PDF 为

$$f_{G_2}(x)=\frac{1}{\rho\Gamma(M)}\left(\frac{x}{\rho}\right)^{M-1}\mathrm{e}^{-\frac{x}{\rho}} \tag{24}$$

由式(14)、(23)和(24)可知目的节点接收 SINR 的 CDF 为

$$F_{\tilde{\gamma}_2}(x)=P_{\tilde{\gamma}_2}\left\{\frac{G_1G_2}{G_1+G_2+\rho U+1}<x\right\} \tag{25}$$

推导可得系统传输中断概率为(推导过程见附录 C)

$$F_{\tilde{\gamma}_2}(x)=1-2^BL_4(x)+L_3(x) \tag{26}$$

其中

$$L_3(x)=\frac{\mathrm{e}^{-\frac{x}{\rho(1-\delta)}}\mathrm{e}^{-\frac{x}{\rho}}}{\rho^M\Gamma(M)}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1}\sum_{m=0}^{k}\binom{M-1}{l}\cdot\binom{k}{m}\frac{(\delta^{k-M+1}-1)}{k!(1-\delta)^k\rho^k}(1+\rho U+x)^m\cdot 2x^{l+k}\left(\frac{(1+\rho U+x)x}{(1-\delta)}\right)^{\frac{M-l-m}{2}}\cdot K_{M-l-m}\left(\frac{2}{\rho}\sqrt{\frac{(1+\rho U+x)x}{(1-\delta)}}\right) \tag{27}$$

$$L_4(x)=\frac{\mathrm{e}^{-\frac{2x}{\rho}}}{\rho^M\Gamma(M)}\sum_{l=0}^{M-1}\binom{M-1}{l}2x^{M-l-1}\cdot[(1+\rho U+x)x]^{\frac{l+1}{2}}K_{l+1}\left(\frac{2\sqrt{(1+\rho U+x)x}}{\rho}\right) \tag{28}$$

故可得到目标容量为 C_0 的系统传输中断概率

$$P_{\text{out}} = F_{\tilde{\gamma}_2}(2^{2C_0}-1) = 1 - 2^B L_4(2^{2C_0}-1) + L_3(2^{2C_0}-1) \tag{29}$$

由式(27)、(28)和(29)可知,系统传输中断概率 P_{out} 是 C_0、M、ρ 和 B 的函数.当 C_0、M 和 ρ 给定时,由式(29)知 P_{out} 与 $F_{\tilde{\gamma}_2}(x)$ 关于 B 的单调性相同,又由式(42)知 $F_{\tilde{\gamma}_2}(x)$ 与 $F_{G_1}(x)$ 关于 B 的单调性相同,由式(23)及附录 B 知 $F_{G_1}(x)$ 与 $F_{C^*}(x)$ 同为关于 B 的单调减函数,故 P_{out} 是 B 的单调减函数.这是由于反馈比特数越大,则信道估计越精确,量化误差夹角 θ 越小,从而使 S-R 信道的波束成形向量 w_{SR} 越准确.故可得出结论:反馈比特数越大,传输中断概率越小,即系统可靠性越高.

类似地,我们亦推得已知完全 CSI 情况下非可信中继模型接收 SINR 的 CDF 如下:

$$\begin{aligned} F_{\tilde{\gamma}_2}^{*}(x) &= 1 - \frac{\mathrm{e}^{-\frac{2x}{\rho}}}{\rho^M \Gamma(M)} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} \sum_{m=0}^{k} \binom{M-1}{l} \\ &\cdot \binom{k}{m} \frac{(1+\rho U+x)^m}{k!\ \rho^k} ((1+\rho U+x)x)^{\frac{M-l-m}{2}} \\ &\cdot 2x^{l+k} K_{M-l-m}\left(\frac{2}{\rho}\sqrt{(1+\rho U+x)x}\right) \end{aligned} \tag{30}$$

故可得到不考虑有限反馈时目标容量为 C_0 的系统中断概率

$$P_{\text{out}}^{*} = F_{\tilde{\gamma}_2}^{*}(2^{2C_0}-1) \tag{31}$$

3.3 最优反馈比特选择

综上所述,安全中断概率和传输中断概率分别是反馈比特数 B 的单调增函数和单调减函数.因此,在选择反馈比特数 B 时,必须同时考虑 B 对系统安全性和可靠性的影响.

首先考虑系统的传输中断概率.设存在一个阈值 $\varepsilon>0$,当目标节点的接收 SINR 值 $\tilde{\gamma}_2<\varepsilon$ 时,系统传输中断;而当 $\tilde{\gamma}_2>\varepsilon$ 时,系统则能够正常接收[7].由此可对反馈比特数 B 进行约束.

式(14)中,给定 ρ 时,$\tilde{\gamma}_2$ 的均值为

$$E[\tilde{\gamma}_2] = E\left[\rho\frac{ABC}{AC+B+U+\frac{1}{\rho}}\right] \geqslant \frac{E[AC]\rho U}{E[AC]+2U+\frac{1}{\rho}}$$

$$\geqslant \frac{(1-2^{-\frac{B}{M-1}})\rho U^2}{(1-2^{-\frac{B}{M-1}})U+2U+\frac{1}{\rho}} \geqslant \varepsilon \tag{32}$$

其中第一个不等式为简森不等式[3],第二个不等式为利用式(7)取下界所得.由 $1>(1-2^{-\frac{B}{M-1}})>0$ 得

$$\frac{\rho U^2}{3U+\frac{1}{\rho}} > \frac{(1-2^{-\frac{B}{M-1}})\rho U^2}{(1-2^{-\frac{B}{M-1}})U+2U+\frac{1}{\rho}} > 0$$

故得到阈值 ε 的取值范围为

$$0<\varepsilon<\frac{\rho U^2}{3U+\frac{1}{\rho}} \tag{33}$$

对式(32)的不等式进行简化,可得反馈比特数下界:

$$B \geqslant -(M-1)\log_2\left(1-\frac{\left(2U+\frac{1}{\rho}\right)\varepsilon}{\rho U^2-\varepsilon U}\right) \tag{34}$$

由式(32)可知,当反馈比特数大于该下界时,接收 SINR 的均值将大于所设置阈值 ε,从而改善系统的传输可靠性.而由式(19)已知系统的安全中断概率是反馈比特数 B 的单调增函数,反馈比特数应尽可能地小,以提高系统的安全性.同时考虑系统的可靠性和安全性,可知最优反馈比特数为式(34)的下界:

$$\tilde{B} = \left\lceil -(M-1)\log_2\left(1-\frac{\left(2U+\frac{1}{\rho}\right)\varepsilon}{\rho U^2-\varepsilon U}\right)\right\rceil \tag{35}$$

其中$\lceil\cdot\rceil$符号表示上取整函数.显然,在 ε 的取值范围内,$\tilde{B}$ 是 ε 的不减函数.因此,系统最优反馈比特数 $\tilde{B}$ 能够根据阈值 ε 由式(35)直接计算得到,从而实现最优反馈比特数的自适应调整,以满足实际需要.

4 仿真结果与讨论

本节针对图 1 中双跳半双工非可信中继系统模型在平坦瑞利衰落信道下进行仿真,完成对上述理论分析结果的验证,其中 S 节点与 D 节点的天线数 $M=4$,R 节点为单天线,每个节点的发送功率均为 P,噪声功率归一化为 $\sigma^2=1$.

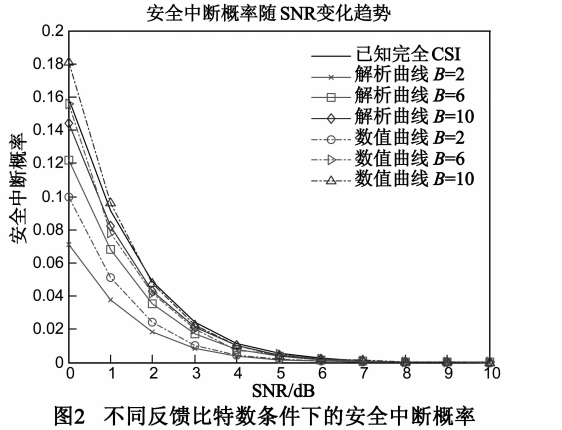

图2　不同反馈比特数条件下的安全中断概率

图 2 所示为选择不同反馈比特数情况下,安全中断概率随 SNR(即 ρ)变化曲线图,其中有限反馈情况下的解析曲线由式(19)获得,已知完全 CSI 情况的曲线由式(22)获得.从图中可以看到,随反馈比特数的增加,安全中断概率上升,即系统安全性能变差,与前文的讨论结果相符,验证了安全中断率关于反馈比特数的单调性.同时可得,随着反馈比特数的逐渐变大,安全中断概率

间距逐渐变小,即逐渐收敛.这是由式(6)所决定的:随着 B 的逐渐增大,量化误差夹角分布将逐渐集中于 0,量化误差也就越小,最终安全中断概率收敛于获得完全 CSI 的情况下.而对于固定的 B,安全中断概率随 SNR 的增大而变小.这是因为目标节点的接收信号经历了两个时隙的多跳传输,相对于窃听中继的单跳接收,噪声对接收者的影响更大,因此高性噪比环境有益于系统安全性.从图 2 中亦可看出,解析曲线和数值曲线随着 SNR 的增加趋于吻合,在 SNR 大于 4dB 时重合,验证了推导结果的正确性.在 SNR 小于 4dB 时,两类曲线之间存在差异,主要由两个方面的原因所导致.首先是式(17)的简化带来一定的误差,其次是式(19)的推导中对第一时隙 *R-D* 信道系数仅采用其统计平均值,这个差异在噪声影响较大的低 SNR 环境下更明显.

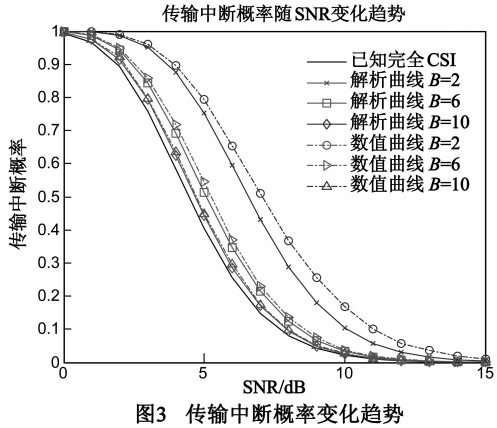

图3 传输中断概率变化趋势

图 3 给出了不同反馈比特数情况下,系统传输中断概率随 SNR 变化的曲线,其中有限反馈情况下的解析曲线由式(29)获得,已知完全 CSI 情况的曲线由式(31)获得.计算传输中断概率时,设置目标速率 $C_0 = 1$bps/Hz.从图中可以看到,随着反馈比特数的增加,传输中断概率下降,即系统可靠性提高,与前文讨论的结果相符,验证了传输中断率关于反馈比特数的单调递减性.然而,随着反馈比特数的增加,反馈比特数对传输中断概率的贡献逐渐减少,最终趋于收敛,其收敛原因与图 2 的收敛原因类似.对于任一给定的 B,传输中断概率随 SNR 的增大而变小,因此高 SNR 环境有益于系统可靠性.从图 3 中亦可看出,解析曲线和数值曲线随着 SNR 的增加趋于吻合,验证了推导结果的正确性.两曲线之间的差异随着反馈比特数的增加而减少,并在反馈比特数为 10 时两曲线完全重合.这是因为反馈比特数越少,估计误差则越大,这是在对第一时隙 *R-D* 信道系数取了统计平均的情况下所导致的,从而造成了解析值与实际数值的差异.

图 4 给出了不同接收 SINR 阈值 ε 下最优反馈比特数的选择变化曲线,其中下界由式(34)给出,且 SNR 固定取值为 10dB.很显然,反馈比特数下界随着 ε 的增加而增加,从而验证了前文所推导的反馈比特数与阈值的单调递增关系.当阈值 ε 的取值接近式(33)给出的最大取值时,反馈比特数下界增加得非常快.然而在实际应用场合,若接收 SINR 阈值适当,由式(35)将自适应获得一个易于实现的最优反馈比特数.

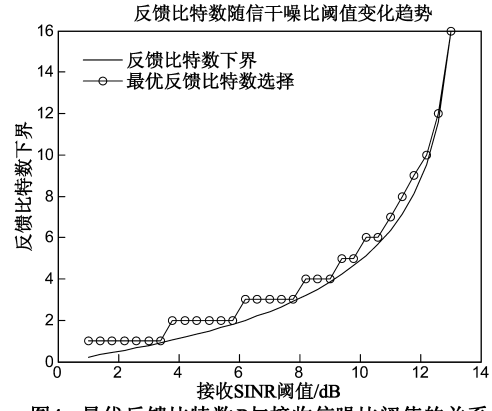

图4 最优反馈比特数B与接收信噪比阈值的关系

附录 A

推导安全中断概率闭合表达式:

由式(18)可知

$$\begin{aligned} P\{\tilde{\gamma}_1 > \tilde{\gamma}_2\} &= P\left\{C^* < G^* - U - \frac{1}{\rho}\right\} \\ &= \int_{U+\frac{1}{\rho}}^{\infty} F_{C^*}\left(t - U - \frac{1}{\rho}\right) f_{G^*}(t)\mathrm{d}t \\ &= \int_0^{\infty} F_{C^*}(t) f_{G^*}\left(t + U + \frac{1}{\rho}\right)\mathrm{d}t \end{aligned} \tag{36}$$

$$\begin{aligned} &= \underbrace{\int_0^{\infty} (1 - 2^B e^{-t}) f_{G^*}\left(t + U + \frac{1}{\rho}\right)\mathrm{d}t}_{I_2} \\ &+ \underbrace{\int_0^{\infty} e^{-\frac{t}{1-\delta}} \sum_{k=0}^{M-1} \frac{(\delta^{k-M+1} - 1)t^k}{k!(1-\delta)^k} f_{G^*}\left(t + U + \frac{1}{\rho}\right)\mathrm{d}t}_{I_3} \end{aligned} \tag{37}$$

由式(16)和式(37)可得到 I_2

$$\begin{aligned} I_2 &= 1 - \frac{2^B e^{-\frac{\rho K+1}{\rho^2 U}}}{(\rho U)^M \Gamma(M)} \int_0^{\infty} \sum_{i=0}^{M-1} \binom{M-1}{i} \\ &\quad \cdot \left(U + \frac{1}{\rho}\right)^{M-1-i} t^i e^{-\frac{\rho U+1}{\rho U}t}\mathrm{d}t \\ &\overset{(a)}{=} 1 - \frac{2^B e^{-\frac{\rho U+1}{\rho^2 U}}}{(\rho U)^M \Gamma(M)} \sum_{i=0}^{M-1} \binom{M-1}{i} \\ &\quad \cdot \left(U + \frac{1}{\rho}\right)^{M-1-i} \left(\frac{\rho U}{1+\rho U}\right)^{i+1} \Gamma(i+1) \end{aligned} \tag{38}$$

由式(16)和式(37)可得到 I_3

$$I_3 = \sum_{k=0}^{M-1} \frac{(\delta^{k-M+1}-1)e^{-\frac{\rho U+1}{\rho^2 U}}}{k!(1-\delta)^k(\rho U)^M\Gamma(M)} \cdot \int_0^\infty \sum_{i=0}^{M-1}\binom{M-1}{i}\left(U+\frac{1}{\rho}\right)^{M-1-i} t^{k+i}e^{-\frac{1-\delta+\rho U}{\rho U(1-\delta)}t}\mathrm{d}t$$

$$\overset{(b)}{=} \sum_{k=0}^{M-1} \frac{(\delta^{k-M+1}-1)e^{-\frac{\rho U+1}{\rho^2 U}}}{k!(1-\delta)^k(\rho U)^M\Gamma(M)} \sum_{i=0}^{M-1}\binom{M-1}{i} \cdot \left(U+\frac{1}{\rho}\right)^{M-1-i}\left(\frac{1-\delta+\rho U}{(1-\delta)\rho U}\right)^{k+i+1}\Gamma(k+i+1) \tag{39}$$

其中(a)和(b)使用了文献[11]中的

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\mathrm{d}t$$

故由式(37)、(38)和(39),得到安全中断概率

$$P\{\tilde{\gamma}_1 > \tilde{\gamma}_2\} = 1 - P\{\tilde{\gamma}_1 < \tilde{\gamma}_2\} = 2^B I_4 - I_3 \tag{40}$$

其中

$$I_4 = \frac{e^{-\frac{\rho U+1}{\rho^2 U}}}{(\rho U)^M\Gamma(M)}\sum_{i=0}^{M-1}\binom{M-1}{i} \cdot \left(U+\frac{1}{\rho}\right)^{M-1-i}\left(\frac{\rho U}{1+\rho U}\right)^{i+1}\Gamma(i+1) \tag{41}$$

附录 B

证明 $P\{\tilde{\gamma}_1 < \tilde{\gamma}_2\}$是 B 的单调增函数:

由文献[17]可知 $C^* = AC = \| \boldsymbol{h}_{SR}^H \|^2 \cos^2\theta$ 的 CDF 为

$$\begin{aligned} F_{C^*}(x) &= P(\| \boldsymbol{h}_{SR}^H \|^2 \cos^2\theta \leqslant x) \\ &= 1 - P\left(\sin^2\theta \leqslant 1 - \frac{x}{C}\right) \\ &= 1 - \int_0^t F_{\sin^2\theta}\left(1-\frac{x}{t}\right) f_C(t)\,\mathrm{d}t \end{aligned} \tag{42}$$

由式(5)可知 $F_{\sin^2\theta}(x)$是 B 的单调增函数,且 $f_C(x)$与 B 无关,故式(41)即 $F_{C^*}(x)$是 B 的单调减函数.由式(16)可知 $f_{C^*}(x)$与 B 无关,故由式(36)可知 $P\{\tilde{\gamma}_1 > \tilde{\gamma}_2\}$与 $F_{C^*}(x)$关于 B 的单调性相同,即 $P\{\tilde{\gamma}_1 > \tilde{\gamma}_2\}$是关于 B 的单调减函数,故 $P\{\tilde{\gamma}_1 < \tilde{\gamma}_2\}$是 B 的单调增函数.

附录 C

推导系统传输中断概率闭合表达式:

由式(25)可知

$$\begin{aligned} F_{\tilde{\gamma}_2}(x) &= P_{\tilde{\gamma}_2}\left\{\frac{G_1G_2}{G_1+G_2+\rho U+1} < x\right\} = F_{G_2}(x) \\ &+ \int_x^\infty F_{G_1}\left(\frac{(1+\rho U)x+ux}{u-x}\right) f_{G_2}(u)\,\mathrm{d}u \\ &= F_{G_2}(x) + \underbrace{\int_0^\infty F_{G_1}\left(\frac{(1+\rho U+x)x}{t}+x\right) f_{G_2}(x+t)\,\mathrm{d}t}_{L_1(x)} \end{aligned} \tag{43}$$

由式(23)、(24)和(43)可得 $L_1(x)$

$$L_1(x) = \int_0^\infty f_{G_2}(x+t)\,\mathrm{d}t + L_3(x) - \underbrace{\int_0^\infty 2^B e^{-\left(\frac{(1+\rho U+x)x}{\rho t}+\frac{x}{\rho}\right)} f_{G_2}(x+t)\,\mathrm{d}t}_{L_2(x)} \tag{44}$$

其中

$$L_3(x) = \int_0^\infty e^{-\frac{\left(\frac{(1+\rho U+x)x}{t}+x\right)}{\rho(1-\delta)}} \sum_{k=0}^{M-1} \frac{\left(\frac{(1+\rho U+x)x}{t}+x\right)^k}{k!(1-\delta)^k\rho^k} \cdot (\delta^{k-M+1}-1) f_{G_2}(x+t)\,\mathrm{d}t \tag{45}$$

由式(24)和(43)可得 $L_2(x)$

$$\begin{aligned} L_2(x) &= \int_0^\infty 2^B e^{-\left(\frac{(1+\rho U+x)x}{\rho t}\right)} e^{-\frac{x}{\rho}} \cdot \frac{1}{\rho^M\Gamma(M)}(x+t)^{M-1}e^{-\frac{x}{\rho}}e^{-\frac{t}{\rho}}\mathrm{d}t \\ &= \frac{2^B e^{-\frac{2x}{\rho}}}{\rho^M\Gamma(M)}\sum_{l=0}^{M-1}\binom{M-1}{l}x^{M-l-1} \cdot \int_0^\infty t^l e^{-\left(\frac{(1+\rho U+x)x}{\rho t}\right)} e^{-\frac{t}{\rho}}\mathrm{d}t \overset{(c)}{=} 2^B L_4(x) \end{aligned} \tag{46}$$

其中

$$L_4(x) = \sum_{l=0}^{M-1}\binom{M-1}{l}[(1+\rho U+x)x]^{\frac{l+1}{2}} \cdot \frac{2x^{M-l-1}e^{-\frac{2x}{\rho}}}{\rho^M\Gamma(M)}K_{l+1}\left(\frac{2\sqrt{(1+\rho U+x)x}}{\rho}\right) \tag{47}$$

由式(24)和(45)可得 $L_3(x)$

$$\begin{aligned} L_3(x) &= \int_0^\infty \sum_{k=0}^{M-1} \frac{\left(\frac{(1+\rho U+x)x}{t}+x\right)^k}{k!(1-\delta)^k\rho^k} \cdot (\delta^{k-M+1}-1)e^{-\frac{x}{\rho(1-\delta)}}e^{-\frac{(1+\rho U+x)x}{\rho(1-\delta)t}} \\ &\cdot \frac{1}{\rho^M\Gamma(M)}(x+t)^{M-1}e^{-\frac{x}{\rho}}e^{-\frac{t}{\rho}}\mathrm{d}t \\ &= \frac{e^{-\frac{x}{\rho(1-\delta)}}e^{-\frac{x}{\rho}}}{\rho^M\Gamma(M)}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1}\sum_{m=0}^{k}\binom{M-1}{l} \cdot \binom{k}{m}\frac{(\delta^{k-M+1}-1)}{k!(1-\delta)^k\rho^k}(1+\rho U+x)^m \\ &\cdot x^{l+k}\int_0^\infty t^{M-l-m-1}e^{-\frac{(1+\rho U+x)x}{\rho(1-\delta)t}}e^{-\frac{t}{\rho}}\mathrm{d}t \\ &\overset{(d)}{=} \frac{2e^{-\frac{x}{\rho(1-\delta)}}e^{-\frac{x}{\rho}}}{\rho^M\Gamma(M)}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1}\sum_{m=0}^{k}\binom{M-1}{l} \cdot \binom{k}{m}\frac{(\delta^{k-M+1}-1)}{k!(1-\delta)^k\rho^k}(1+\rho U+x)^m \end{aligned}$$

$$\cdot x^{l+k}\left(\frac{(1+\rho U+x)x}{(1-\delta)}\right)^{\frac{M-l-m}{2}} \cdot K_{M-l-m}\left(\frac{2}{\rho}\sqrt{\frac{(1+\rho U+x)x}{(1-\delta)}}\right) \quad (48)$$

其中(c)和(d)使用了文献[18]中的积分方法,$K_v(\cdot)$是 v 阶贝塞尔第二类修正函数.

由式(43)~式(48)即可得到 $F_{\tilde{\gamma}_2}(x)$的闭合表达式:

$$F_{\tilde{\gamma}_2}(x) = 1 - 2^B L_4(x) + L_3(x) \quad (49)$$

参考文献

[1] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355 – 1387.

[2] Zhang R, Song L, Han Z, et al. Physical layer security for two-way untrusted relaying with friendly jammers[J]. IEEE Transactions on Vehicular Technology, 2012, 61(8): 3693 – 3704.

[3] 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.

[4] Shen Y, Jiang X, Ma J, et al. Secure and Reliable Transmission with Cooperative Relays in Two Hop Wireless Networks[M]. Information Technology Convergence, Springer Netherlands, 2013. 253: 397 – 406.

[5] Zou Y, Wang X, Shen W. Optimal relay selection for physical-layer security in cooperative wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10): 2099 – 2111.

[6] Huang J, Swindlehurst A L. Cooperative jamming for secure communications in MIMO relay networks[J]. IEEE Transactions on Signal Processing, 2011, 59(10): 4871 – 4884.

[7] Krikidis I, Thompson J S, McLaughlin S. Relay selection for secure cooperative networks with jamming[J]. IEEE Transactions on Wireless Communications, 2009, 8(10): 5003 – 5011.

[8] Chen J, Zhang R, Song L, et al. Joint relay and jammer selection for secure two-way relay networks[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 310 – 320.

[9] Jindal N. MIMO broadcast channels with finite-rate feedback [J]. IEEE Transactions on Information Theory, 2006, 52(11): 5045 – 5060.

[10] Yoo T, Jindal N, Goldsmith A. Multi-antenna downlink channels with limited feedback and user selection[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(7): 1478 – 1491.

[11] Erlin Z, Shihua Z, Zhong Z, et al. On the performance of amplify-and-forward relay systems with limited feedback beamforming[J]. IEICE Transactions on Communications, 2008, 91(6): 2053 – 2057.

[12] Chen X, Yin R. Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback[J]. IEEE Transactions on Wireless Communications, IEEE, 2013, 2(5): 503 – 506.

[13] Li N, Tao X F, Xu J. Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback[J]. IEEE Transactions on Communication Letters, 2014, 18(6): 969 – 972.

[14] Bashar S, Ding Z, Li G Y. On secrecy of codebook-based transmission beamforming under receiver limited feedback [J]. IEEE Transactions on Wireless Communications, 2011, 10(4): 1212 – 1223.

[15] Gerbracht S, Scheunert C, Jorswieck E A. Secrecy outage in MISO systems with partial channel information[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 704 – 716.

[16] Tekin E. The Gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming[A]. Proceedings of the IEEE Information Theory and Applications Workshop (ITA) [C]. San Diego, California, 2007. 404 – 413.

[17] Pei M, Ma D, Wei J. Adaptive limited feedback for MISO wiretap channels with cooperative jamming[J]. IEEE Transactions on Signal Processing, 2013, 62(4): 993 – 1004.

[18] Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products[M]. New York: Academic Press, 1965.

作者简介

吴亚峰 男,1990 年生于江西南昌,硕士研究生.主要研究方向为协同中继网络物理层安全通信和有限反馈技术.

E-mail: windsnow263@163.com

赵 睿(通信作者) 男,1980 年生于江苏扬州,博士,副教授,研究领域为无线通信信号处理、协作通信和物理层安全通信.

E-mail: rzhao@hqu.edu.cn

贺玉成 男,1964 年生于山西太原,博士,教授.主要研究方向为无线通信、信道编码、协作无线通信等.

E-mail: yucheng.he@hqu.edu.cn

谢维波 男,博士,教授,硕士生导师,主要研究方向为现代信号处理、人工智能和嵌入式系统等.

E-mail: xwblxf@hqu.edu.cn