研究与开发

MF 中继选择系统的物理层安全性能

程英，李光球，沈静洁，韦亮
（杭州电子科技大学通信工程学院，浙江 杭州 310018）

摘　要：针对合谋窃听场景下单天线多中继修改转发（MF）协作无线系统的安全性能较差问题，提出一种合谋窃听场景下联合源节点发送天线选择（TAS）和多中继选择的 MF 协作物理层安全系统，考虑最优的最大化主信道信噪比（SNR）和次优的最大化源节点−中继节点链路 SNR 两种中继选择方案，推导其安全中断概率（SOP）和遍历安全容量（ESC）的解析表达式。最优或次优中继选择的 MF 安全中继系统的 SOP 和 ESC 的数值计算结果与仿真结果相吻合，验证了上述理论分析的正确性；同时也表明源节点发射天线数和中继节点数越多、窃听节点数越少，最优或次优中继选择的 MF 安全中继系统的物理层安全性能越好。

关键词：发送天线选择；中继选择；物理层安全；修改转发；安全中断概率；遍历安全容量
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021213

Physical layer security performance of MF relay selection systems

CHENG Ying, LI Guangqiu, SHEN Jingjie, WEI Liang
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Aimed at the poor security performance of single antenna multi-relay modify-and-forward (MF) cooperative wireless systems in collusion eavesdropping scenario, MF cooperative physical layer security systems combining source node transmit antenna selection (TAS) and multi-relay selection in collusion eavesdropping scenario were proposed. Two relay selection schemes were considered, namely, the optimal maximization of the main channel signal-to-noise ratio (SNR) and the suboptimal maximization of the source-relay link SNR. The closed-form expressions of the secrecy outage probability (SOP) and ergodic secure capacity (ESC) for the above MF cooperative wireless systems were derived. The numerical results of SOP and ESC of MF secure relay systems with optimal or suboptimal relay selection were consistent with the simulation results, which verifies the correctness of the above theoretical analysis. It also shows that the more the number of transmit antennas at the source node and relay nodes, and the less the number of eavesdropping nodes, the better the physical layer security performance of MF secure relay systems with optimal or suboptimal relay selection.

Key words: transmit antenna selection, relay selection, physical layer security, modify-and-forward, secrecy outage probability, ergodic secrecy capacity

收稿日期：2021−06−18；修回日期：2021−09−13
通信作者：李光球，gqli@hdu.edu.cn

1 引言

译码转发（decode-and-forward，DF）中继协作无线系统的物理层安全是当前无线通信的一个重要研究方向。当源节点与目的节点之间的信道质量很差时，可以利用 DF 中继协作无线系统进行信息安全传输[1]。文献[2]推导了毫米波 DF 中继协作系统的安全中断概率（secrecy outage probability，SOP）解析表达式。文献[3]推导了机会式传输策略下自适应 DF 中继协作系统的 SOP 闭合表达式。采用中继选择可以有效提升协作无线系统的物理层安全性能[4]。文献[5]分别研究了采用最优中继选择的放大转发（amplify-and-forward，AF）与 DF 中继协作无线系统的物理层安全性能。文献[6]推导了最大化源节点–目的节点信干噪比准则下的联合源节点和中继节点选择的 DF 中继系统 SOP 的近似表达式。发送天线选择（transmit antenna selection，TAS）具有实现复杂度低、性能好的优点[7]，其与中继选择相结合可以进一步提升协作无线系统的安全性。文献[8]研究了源节点和中继节点均采用 TAS 和功率分配技术的两跳 DF 中继系统的物理层安全性能。文献[9]分别推导了 DF 中继协作系统在最大–最小准则和部分信干噪比中继选择下的 SOP 近似表达式。

文献[10-11]对 DF 协议进行改进，提出了修改转发（modify-and-forward，MF）协议。在 MF 协作系统中，中继节点使用与目的节点共享的密钥对接收、解码得到的信息进行修改后再转发，能够避免将合法信号泄露到窃听节点，与 DF 协议相比，MF 协议显著提升了协作无线系统的物理层安全性能；当不作修改时，MF 协议可退化为 DF 协议[10]。文献[11]推导了两跳 MF 中继系统的 SOP 闭合表达式，并与传统 DF 中继协作系统相比较，结果表明 MF 中继系统的 SOP 始终小于 DF 中继系统的 SOP。文献[12]研究了机会安全传输协议下为实现两跳 MF 中继系统最低 SOP 的最佳传输策略。文献[13]推导了多窃听者场景下 MF 中继选择系统的 SOP 和遍历安全容量（ergodic secrecy capacity，ESC）的闭合表达式。

借鉴 TAS 和中继选择可以改善 DF 中继协作无线系统的物理层安全性能，为了改善单天线多中继 MF 协作无线系统的物理层安全性能，本文提出一种合谋窃听场景下源节点采用联合 TAS 和多中继选择的 MF 无线安全系统，分别考虑中继节点采用最大化主信道信噪比（signal to noise ratio，SNR）的最优中继选择方案和最大化源节点–中继节点链路 SNR 的次优中继选择方案，推导其 SOP 和 ESC 的精确表达式，研究 MF 系统中的各参数对其物理层安全性能的影响。

2 系统模型

考虑瑞利衰落信道上合谋窃听场景下采用联合源节点 TAS 和多中继选择的 MF 无线安全系统，如图 1 所示。系统由源节点 S、K 个中继节点 R_k（$k=1,\cdots,K$）、目的节点 D 以及 N 个被动窃听节点 E_n（$n=1,\cdots,N$）组成，S 配备 M 根发射天线，R_k、D 和 E_n 均配备单根天线，中继节点 R_k 均采用 MF 协议，且有如下假设。

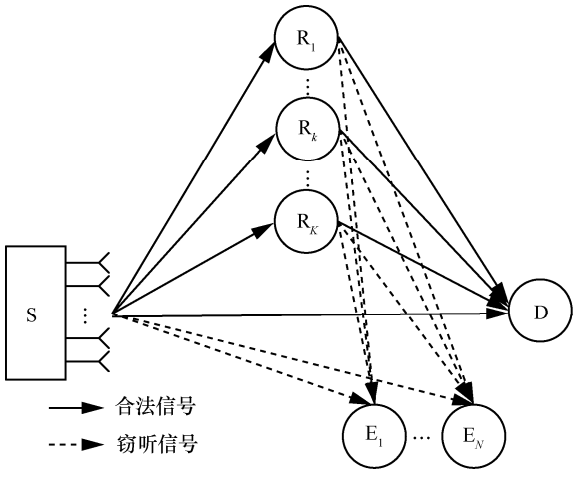

图 1 中继选择 MF 系统的物理层安全模型

（1）源节点与目的节点、窃听节点之间均存在直达链路。

（2）K 个中继节点的发射功率均相等，表示为 p_{R}。

（3）主信道由 $\mathrm{S}\to\mathrm{R}_k$、$\mathrm{R}_k\to\mathrm{D}$、$\mathrm{S}\to\mathrm{D}$ 链路组成，窃听信道由 $\mathrm{S}\to\mathrm{E}_n$、$\mathrm{R}_k\to\mathrm{E}_n$ 链路组成。S 的第 m 根天线至 R_k/D/E_n、R_k 至 D、R_k 至 E_n 链路的信道增益分别表示为 h_{mk}、$h_{m\mathrm{D}}$、h_{mn}、$h_{k\mathrm{D}}$、h_{kn}，均服从复高斯分布 $\mathrm{CN}(0,1)$。

（4）R_k、D、E_n 的接收天线上的加性白高斯噪声相互独立，且分别服从复高斯分布 $\mathrm{CN}(0,\sigma_k^2)$、$\mathrm{CN}(0,\sigma_{\mathrm{D}}^2)$、$\mathrm{CN}(0,\sigma_n^2)$。

假定如图 1 所示的中继选择 MF 系统工作在半双工模式，其信号传输在两跳内完成，在第一跳内，S 广播信号 x，R_k 和 D 均能接收 x，同时，E_n 也能窃听 x。令 γ_{mt} 为 S 第 m（$1\leqslant m\leqslant M$）根发射天线发送信号时节点 t 的瞬时输出 SNR，$t\in(k,\mathrm{D},n)$，分别表示 R_k、D、E_n 的瞬时输出 SNR，有 $\gamma_{mt}=\left|h_{mt}\right|^2/\alpha_t$，其中，$\alpha_t=\sigma_t^2/p_{\mathrm{S}}$，$p_{\mathrm{S}}$ 表示 S 的发射功率。

选择使 $\gamma_{m\mathrm{D}}$ 为最大的 S 的第 m^* 根天线发送信号，其值为 $\gamma_{m^*\mathrm{D}}=\max_{1\leqslant m\leqslant M}\gamma_{m\mathrm{D}}$，$\gamma_{m^*\mathrm{D}}$ 的概率密度函数（probability density function，PDF）为：

$$f_{\gamma_{m^*\mathrm{D}}}(\gamma)=\sum_{j=1}^{M}\binom{M}{j}(-1)^{j-1}\frac{j}{\alpha_{\mathrm{D}}}\exp\left(-\frac{j}{\alpha_{\mathrm{D}}}\gamma\right)\tag{1}$$

在第二跳内，被选择的 R_{k^*} 采用 MF 协议先解码第一跳内接收的信号并将其修改为 $\hat{x}$，然后将 $\hat{x}$ 转发给 D，D 在第二跳的瞬时输出 SNR 为 $\gamma_{k^*\mathrm{D}}=\left|h_{k^*\mathrm{D}}\right|^2/\beta$，其中，$\beta=\sigma_{\mathrm{D}}^2/p_{\mathrm{R}}$。

$\hat{x}$ 与原始信号 x 的差值 δ 根据 R_{k^*} 和 D 之间的物理信道状态信息（channel state information，CSI）获得，由于信道的互易性，D 可以获得 δ，从而能够恢复出原始信号。当 E_n 与 D 之间的距离超过半波长时，R_{k^*} 和 E_n 之间的窃听信道就独立于 R_{k^*} 和 D 之间的合法信道[14]，由于 E_n 无法获得 δ，因此，R_{k^*} 和 D 之间的安全传输便得以保障。

D 运用最大比合并（maximum ratio combining，MRC）方法合并第一跳和第二跳的接收信号，则合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的主信道容量为[13]：

$$C_{\mathrm{D}}=\min\left\{\frac{1}{2}\mathrm{lb}\left(1+\gamma_{m^*k^*}\right),\frac{1}{2}\mathrm{lb}\left(1+\gamma_{m^*\mathrm{D}}+\gamma_{k^*\mathrm{D}}\right)\right\}\tag{2}$$

由式（2）可以看出，MF 协议与 DF 协议在第一跳的传输是相同的，仅在第二跳对窃听者的影响不同。因此，MF 协议与 DF 协议的主信道信道容量是相同的。

E_n 无法解码 R_{k^*} 修改后的信息，只能窃听 S 广播的信息。考虑最坏的窃听场景——合谋窃听，每个 E_n 可以共享各自窃听的信息，因此，可以使用 MRC 共同解码窃听到的信息[15]，此时，合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的窃听信道容量可以表示为：

$$C_{\mathrm{E}}=\frac{1}{2}\mathrm{lb}\left(1+\gamma_{m^*\mathrm{E}}\right)\tag{3}$$

其中，$\gamma_{m^*\mathrm{E}}=\sum_{n=1}^{N}\gamma_{m^*n}$，假设 h_{m^*n} 均独立同分布，根据文献[13]的式（8）可得，采用合谋窃听的窃听信道瞬时输出信噪比 $\gamma_{m^*\mathrm{E}}$ 的 PDF 为：

$$f_{\gamma_{m^*\mathrm{E}}}(\gamma)=\frac{\alpha_n^N}{(N-1)!}\gamma^{N-1}\mathrm{e}^{-\alpha_n\gamma}\tag{4}$$

2.1　中继选择方案

对于图 1，考虑如下两个中继选择方案。

（1）最优中继选择

当已知所有主信道的信道状态信息时，选择使式（2）中主信道容量 C_{D} 最大的 R_{k^*} 转发信号，即：

$$k^*=\arg\max_{1\leqslant k\leqslant K}\min\left\{\gamma_{m^*k},\gamma_{m^*\mathrm{D}}+\gamma_{k\mathrm{D}}\right\}\tag{5}$$

其中，$\left|h_{mk}\right|^2$、$\left|h_{k\mathrm{D}}\right|^2$、$\left|h_{m\mathrm{D}}\right|^2$ 为主信道的 CSI。

由于 $\gamma_{m\mathrm{E}}$ 和 R_k 是不相关的，式（5）的中继选择方案为最优中继选择方案，即：

$$k^*=\arg\max_{1\leqslant k\leqslant K}\left\{\frac{1+\min\left\{\gamma_{m^*k},\gamma_{m^*\mathrm{D}}+\gamma_{k\mathrm{D}}\right\}}{1+\gamma_{m^*\mathrm{E}}}\right\}=\arg\max_{1\leqslant k\leqslant K}\min\left\{\gamma_{m^*k},\gamma_{m^*\mathrm{D}}+\gamma_{k\mathrm{D}}\right\}\tag{6}$$

（2）次优中继选择

当只有S→R链路的信道状态信息$|h_{mk}|^2$已知时，选择使S→R链路 SNR 最大的R_{k^*}转发信号，即：

$$k^* = \arg\max_{1\leqslant k\leqslant K}\left\{\gamma_{m^*k}\right\} \tag{7}$$

为叙述方便，将服从参数为λ的指数分布的随机变量 x 记为$x\sim E(\lambda)$，其 PDF 和累积分布函数（cumulative distribution function，CDF）分别为[16]：

$$f(\lambda,x)=\frac{1}{\lambda}\mathrm{e}^{-\frac{x}{\lambda}} \tag{8}$$

$$F(\lambda,x)=1-\mathrm{e}^{-\frac{x}{\lambda}} \tag{9}$$

下面分别推导合谋窃听场景下源节点采用TAS、中继节点采用最优/次优中继选择方案时的MF系统的安全中断概率和遍历安全容量。

2.2 反馈开销分析

假定将D到S的第m根天线、D到R_i以及R_i到S的第m根天线反馈瞬时CSI所需的开销均表示为 T。根据上文的 TAS 准则，获取$|h_{mD}|^2$瞬时CSI所需的反馈开销为MT。

（1）最优中继选择的反馈开销

S需要获得$|h_{m^*k}|^2$、$|h_{kD}|^2$、$|h_{m^*D}|^2$的瞬时CSI，$|h_{kD}|^2$ CSI的获得需要由D经过R_i反馈给S，所需开销为 $2T$，最优中继选择方案总的反馈开销为$(3K+M)T$。若 S 为单天线，则总的反馈开销为$(3K+1)T$。

（2）次优中继选择的反馈开销

S 需要获得$|h_{m^*k}|^2$的瞬时 CSI，则需先进行TAS，获得最优的发送天线，总的反馈开销为$(K+M)T$。若 S 为单天线，则总的反馈开销为KT。

综上，最优中继选择方案的反馈开销高于次优中继选择方案的反馈开销，且具有更高的实现复杂性。

3 安全性能分析

利用式（2）和式（3）可得多窃听者合谋窃听场景下源节点采用 TAS、中继节点采用中继选择方案 l 的 MF 系统的安全容量为：

$$C_l=\max\left\{C_{\mathrm{D}}-C_{\mathrm{E}},0\right\}=\max\left\{\left(\mathrm{lb}\theta_l\right)/2,0\right\} \tag{10}$$

其中，$l\in\{\mathrm{opt},\mathrm{sub}\}$，分别对应最优中继选择方案和次优中继选择方案，$\theta_l=(1+Z_l)/(1+\gamma_{m^*\mathrm{E}})$，$Z_l=\min\{\gamma_{m^*k^*},\gamma_{m^*\mathrm{D}}+\gamma_{k^*\mathrm{D}}\}$。

3.1 安全中断概率

合谋窃听场景下源节点采用TAS的中继选择MF系统的SOP可定义为系统安全容量小于目标安全速率 B 的概率，于是利用文献[17]的式（47）可得采用中继选择方案 l 的 MF 系统的 SOP 为：

$$P_{\mathrm{out}}^{l}=\int_0^{\infty}F_{Z_l}\left((1+\gamma)\gamma_{\mathrm{th}}-1\right)f_{\gamma_{m^*\mathrm{E}}}(\gamma)\mathrm{d}\gamma \tag{11}$$

其中，$\gamma_{\mathrm{th}}=2^{2B}$。

3.1.1 最优中继选择方案的安全中断概率

令 $V_k=\min\{\gamma_{m^*k},\omega+\gamma_{k\mathrm{D}}\}$，$\omega\geqslant 0$，由于$\gamma_{m^*k}\sim E\left(1/\alpha_k\right)$，$\gamma_{k\mathrm{D}}\sim E(1/\beta)$，利用式（9）可推得$V_k$的CDF为：

$$\begin{aligned}&F_{V_k}(v)=\\&1-\left(1-F_{\gamma_{m^*k}}(v)\right)\left(1-F_{\gamma_{k\mathrm{D}}}(v-\omega)\right)=\\&\begin{cases}1-\mathrm{e}^{-\alpha_k v}\mathrm{e}^{-\beta(v-\omega)}, & v>\omega\\ 1-\mathrm{e}^{-\alpha_k v}, & 0<v<\omega\end{cases}\end{aligned} \tag{12}$$

令$V_{\max}=\max\{V_k,k=1,2,\cdots,K\}$，由于$V_k$均相互独立，根据式（12）并利用二项式展开可以推得$V_{\max}$的CDF为：

$$\begin{aligned}&F_{V_{\max}}(v)=\prod_{k=1}^{K}F_{V_k}(v)=\\&\begin{cases}1-\sum_{i=1}^{K}\binom{K}{i}(-1)^{i-1}\mathrm{e}^{i\beta\omega}\mathrm{e}^{-(i\alpha_k+i\beta)v}, & v>\omega\\ 1-\sum_{i=1}^{K}\binom{K}{i}(-1)^{i-1}\mathrm{e}^{-i\alpha_k v}, & 0<v<\omega\end{cases}\end{aligned} \tag{13}$$

由式（1）、式（5）和式（13）可推得 $Z_{\text{opt}}=\min\{\gamma_{m^*k^*},\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}\}$ 的 CDF 为：

$$\text{aligned}F_{Z_{\text{opt}}}(z)=$$

$$\int_0^z F_{V_{\max}}(z)f_{\gamma_{m^*\text{D}}}(\omega)\text{d}\omega+\int_z^\infty F_{V_{\max}}(z)f_{\gamma_{m^*\text{D}}}(\omega)\text{d}\omega=$$

$$1-\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\left(a_1\text{e}^{-b_1z}-a_2\text{e}^{-b_2z}\right)\tag{14}$$

其中，$a_1=\dfrac{i\beta}{i\beta-j\alpha_{\text{D}}}$，$a_2=\dfrac{j\alpha_{\text{D}}}{i\beta-j\alpha_{\text{D}}}$，$b_1=i\alpha_k+j\alpha_{\text{D}}$，$b_2=i\alpha_k+i\beta$。

将式（4）和式（14）代入式（11）可以推得合谋窃听场景下源节点采用 TAS、中继节点采用最优中继选择方案的 MF 系统的 SOP 为：

$$P_{\text{out}}^{\text{opt}}\left(\gamma_{\text{th}}\right)=1-\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\frac{\alpha_n^N}{(N-1)!}\cdot$$

$$\left(a_1\text{e}^{-b_1(\gamma_{\text{th}}-1)}\int_0^\infty\gamma^{N-1}\text{e}^{-(b_1\gamma_{\text{th}}+\alpha_n)\gamma}\text{d}\gamma-\right.$$

$$\left.a_2\text{e}^{-b_2(\gamma_{\text{th}}-1)}\int_0^\infty\gamma^{N-1}\text{e}^{-(b_2\gamma_{\text{th}}+\alpha_n)\gamma}\text{d}\gamma\right)\tag{15}$$

利用文献[18]的式（3.351.3）可将式（15）化简为：

$$P_{\text{out}}^{\text{opt}}\left(\gamma_{\text{th}}\right)=1-\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}\cdot$$

$$(-1)^{i+j}\left(\frac{a_1\text{e}^{-b_1(\gamma_{\text{th}}-1)}}{\left(\gamma_{\text{th}}/s+1\right)^N}-\frac{a_2\text{e}^{-b_2(\gamma_{\text{th}}-1)}}{\left(\gamma_{\text{th}}/t+1\right)^N}\right)\tag{16}$$

其中，$s=\alpha_n/b_1$，$t=\alpha_n/b_2$。

3.1.2　次优中继选择方案的安全中断概率

由式（7）并利用式（9）和二项式展开定理可推得 $\gamma_{m^*k^*}$ 的 CDF 为：

$$F_{\gamma_{m^*k^*}}(\gamma)=\prod_{k=1}^{K}F_{r_{m^*k}}(\gamma)=1-\sum_{i=1}^{K}\binom{K}{i}(-1)^{i-1}\text{e}^{-i\alpha_k\gamma}\tag{17}$$

由于 $\gamma_{k^*\text{D}}\sim E(1/\beta)$，利用式（9）和式（1）以及部分分式展开可推得 $\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}$ 的拉普拉斯变换为：

$$L\left[f_{\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}}(\gamma)\right]=$$

$$\sum_{j=1}^{M}\binom{M}{j}(-1)^{j-1}\frac{\text{j}\alpha_{\text{D}}\beta}{(\gamma+\text{j}\alpha_{\text{D}})(\gamma+\beta)}=$$

$$\sum_{j=1}^{M}\binom{M}{j}(-1)^{j-1}\frac{\text{j}\alpha_{\text{D}}\beta}{\beta-\text{j}\alpha_{\text{D}}}\left(\frac{1}{\gamma+\text{j}\alpha_{\text{D}}}-\frac{1}{\gamma+\beta}\right)\tag{18}$$

对式（18）作拉普拉斯反变换可得 $\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}$ 的 PDF 为：

$$f_{\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}}(\gamma)=\sum_{j=1}^{M}\binom{M}{j}(-1)^{j-1}\frac{j\alpha_{\text{D}}\beta}{\beta-j\alpha_{\text{D}}}\left(\text{e}^{-j\alpha_{\text{D}}\gamma}-\text{e}^{-\beta\gamma}\right)\tag{19}$$

对式（19）中的 γ 进行积分可得 $\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}$ 的 CDF 为：

$$F_{\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}}\left(\gamma\right)=$$

$$1-\sum_{j=1}^{M}\binom{M}{j}(-1)^{j-1}\frac{j\alpha_{\text{D}}\beta}{\beta-j\alpha_{\text{D}}}\left(\frac{1}{j\alpha_{\text{D}}}\text{e}^{-j\alpha_{\text{D}}\gamma}-\frac{1}{\beta}\text{e}^{-\beta\gamma}\right)\tag{20}$$

利用式（17）和式（20）可得 $Z_{\text{sub}}=\min\{\gamma_{m^*k^*},\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}\}$ 的 CDF 为：

$$F_{Z_{\text{sub}}}\left(z\right)=1-\left(1-F_{\gamma_{m^*k^*}}\left(\gamma\right)\right)\left(1-F_{\gamma_{m^*\text{D}}+\gamma_{k^*\text{D}}}\left(\gamma\right)\right)=$$

$$1-\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\left(a_3\text{e}^{-b_1z}-a_4\text{e}^{-b_3z}\right)\tag{21}$$

其中，$a_3=\dfrac{\beta}{\beta-j\alpha_{\text{D}}}$，$a_4=\dfrac{\text{j}\alpha_{\text{D}}}{\beta-\text{j}\alpha_{\text{D}}}$，$b_3=i\alpha_k+\beta$。

采用与式（14）～式（16）相似的推导过程，将式（4）、式（21）代入式（11）可推得合谋窃听场景下源节点采用 TAS、中继节点采用次优中继选择方案的 MF 系统的 SOP 为：

$$P_{\text{out}}^{\text{sub}}\left(\gamma_{\text{th}}\right)=1-\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\cdot$$

$$\left(\frac{a_3\text{e}^{-b_1(\gamma_{\text{th}}-1)}}{\left(\gamma_{\text{th}}/s+1\right)^N}-\frac{a_4\text{e}^{-b_3(\gamma_{\text{th}}-1)}}{\left(\gamma_{\text{th}}/w+1\right)^N}\right)\tag{22}$$

其中，$w=\alpha_n/b_3$。

由式（16）和式（22）可知，合谋窃听场景下源节点采用 TAS、中继节点采用最优/次优中继

选择方案的 MF 系统的 SOP 与源节点发射天线数 M、中继节点数 K、窃听节点数 N 以及各链路平均 SNR 有关。当源节点 S 为单发射天线数时，图 1 系统可退变为文献[13]中的多窃听者场景下中继选择 MF 系统，式（16）和式（22）分别与文献[13]中式（13）和式（20）的结果相同，可见本文结果更具一般性。

3.2 遍历安全容量

合谋窃听场景下源节点采用 TAS、中继节点采用中继选择方案 l 的 MF 系统的 ESC 可表示为[13]：

$$\bar{C}_l = \frac{1}{2\ln 2}\int_1^\infty \ln y f_{\theta_l}(y)\mathrm{d}y \tag{23}$$

其中，$l \in \{\mathrm{opt},\mathrm{sub}\}$，分别对应最优中继选择方案和次优中继选择方案，$f_{\theta_l}(y)$ 为 θ_l 的 PDF 表达式。

3.2.1 最优中继选择方案的遍历安全容量

对式（16）中的 γ_{th} 求导可以推得 θ_{opt} 的 PDF 表达式为：

$$f_{\theta_{\mathrm{opt}}}(y) = \sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\cdot \left(a_2\mathrm{e}^{b_2}t^N\frac{\mathrm{d}}{\mathrm{d}y}\left\{\frac{\mathrm{e}^{-b_2 y}}{[y+t]^N}\right\} - a_1\mathrm{e}^{b_1}s^N\frac{\mathrm{d}}{\mathrm{d}y}\left\{\frac{\mathrm{e}^{-b_1 y}}{[y+s]^N}\right\}\right) \tag{24}$$

将式（24）代入式（23）并利用文献[13]的式（33），可得：

$$\int_1^\infty \ln(x)\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{\mathrm{e}^{-bx}}{(x+a)^N}\right)\mathrm{d}x = \frac{1}{a^N}A(N,a,b) \tag{25}$$

其中，$a>0$，$b>0$，$E_1(z)=\int_1^\infty \frac{\mathrm{e}^{-tz}}{t}\mathrm{d}t$，

$$A(N,a,b) = -E_1(b) + \sum_{k=1}^{N}\frac{1}{a^{1-k}}\cdot \left[\mathrm{e}^{-b}\sum_{n=1}^{k-1}\frac{(n-1)!(-b)^{k-n-1}}{(k-1)!(a+1)^n} + \frac{(-b)^{k-1}}{(k-1)!}\mathrm{e}^{ab}E_1(b(a+1))\right] \tag{26}$$

可推得多窃听者场景下源节点采用 TAS、中继节点采用最优中继选择方案的 MF 系统的 ESC 为：

$$\bar{C}_{\mathrm{opt}} = \frac{1}{2\ln 2}\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\cdot \left(a_2\mathrm{e}^{b_2}A(N,t,b_2) - a_1\mathrm{e}^{b_1}A(N,s,b_1)\right) \tag{27}$$

3.2.2 次优中继选择方案的遍历安全容量

对式(22)中的 γ_{th} 求导可以推得 θ_{sub} 的 PDF 为：

$$f_{\theta_{\mathrm{sub}}}(\theta) = \sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\cdot \left(a_4\mathrm{e}^{b_3}w^N\frac{\mathrm{d}}{\mathrm{d}\theta}\left\{\frac{\mathrm{e}^{-b_3\theta}}{[\theta+w]^N}\right\} - a_3\mathrm{e}^{b_1}s^N\frac{\mathrm{d}}{\mathrm{d}\theta}\left\{\frac{\mathrm{e}^{-b_1\theta}}{[\theta+s]^N}\right\}\right) \tag{28}$$

将式（28）代入式（23）并采用与式（24）～式（27）相同的推导过程可推得多窃听者场景下源节点采用 TAS、中继节点采用次优中继选择方案的 MF 系统的 ESC 为：

$$\bar{C}_{\mathrm{sub}} = \frac{1}{2\ln 2}\sum_{i=1}^{K}\sum_{j=1}^{M}\binom{K}{i}\binom{M}{j}(-1)^{i+j}\cdot \left(a_4\mathrm{e}^{b_3}A(N,w,b_3) - a_3\mathrm{e}^{b_1}A(N,s,b_1)\right) \tag{29}$$

由式（27）和式（29）可知，合谋窃听场景下源节点采用 TAS、中继节点采用最优/次优中继选择方案的 MF 系统的 ESC 与源节点发射天线数 M、中继节点数 K、窃听节点数 N 以及各链路平均 SNR 有关。当源节点 S 为单发射天线数时，图 1 系统可退变为考文献[13]中的多窃听者场景下中继选择 MF 系统，式（27）和式（29）分别与文献[13]中式（36）和式（37）的结果相同，可见本文结果更具一般性。

4 数值计算

下面利用 MATLAB 软件对合谋窃听场景下源节点采用 TAS 的 MF 中继选择系统的安全中断概率和遍历安全容量性能进行数值计算与仿真实验，研究不同参数对上述 MF 中继系统物理层安全性能的影响。若无特殊说明，目标安全速率 B=0.5 bit/(s·Hz)，采用文献[13]的参数设置，图 2～图 5 中各符号的定义见表 1。

表 1　MF 中继选择系统中的各符号定义

符号含义	符号表示
源节点发射天线数	M
窃听节点个数	N
中继节点个数	K
$\mathrm{S}\to\mathrm{R}_k$ 链路平均 SNR	$1/\alpha_k$
$\mathrm{S}\to\mathrm{D}$ 链路平均 SNR	$1/\alpha_{\mathrm{D}}$
$\mathrm{S}\to\mathrm{E}_n$ 链路平均 SNR	$1/\alpha_n$
$\mathrm{R}\to\mathrm{D}$ 链路平均 SNR	$1/\beta$

以窃听节点数 N 为参数的合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的安全中断概率性能曲线如图 2 所示。

（1）当窃听节点的数量 N 较大时，MF 中继系统采用最优/次优中继选择的安全中断概率均增大，这是由于当 N 较大时，共享窃听信息的节点增多，则窃听到的信息量增大，从而增加了窃听信道的容量，而主信道容量保持不变，使得 MF 中继系统安全容量减小，安全中断概率增大。

（2）$\mathrm{S}\to\mathrm{D}$ 链路平均 SNR 越高，MF 中继系统采用最优/次优中继选择方案的安全中断概率均越小，这是由于，根据图 2 中的参数取值可知，$1/\alpha_k$ 和 $1/\beta$ 均随 $1/\alpha_{\mathrm{D}}$ 的增大而增大，而 $\mathrm{S}\to\mathrm{E}_n$ 链路的平均 SNR 是一个定值，所以当 $1/\alpha_{\mathrm{D}}$ 较高时，主信道容量会随之增大，窃听信道容量保持不变，使得 MF 中继系统的遍历安全容量增加。

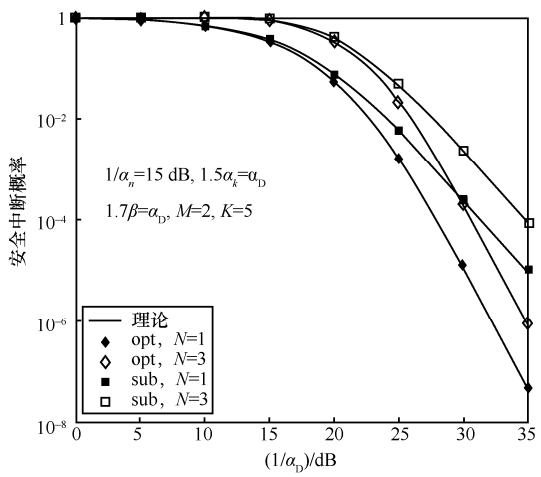

图 2　不同 $1/\alpha_{\mathrm{D}}$ 下 MF 中继系统的安全中断概率

合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的安全中断概率随 $\mathrm{S}\to\mathrm{R}$ 链路平均 SNR 的变化曲线如图 3 所示。

（1）$\mathrm{S}\to\mathrm{R}$ 链路平均 SNR 越高，MF 中继系统采用最优/次优中继选择方案的安全中断概率均越小，且 MF 中继系统的安全中断概率在低信噪比下随 $1/\alpha_k$ 的变化较明显，在高信噪比下，变化较平缓。

（2）增大源节点的发射天线数 M，MF 中继系统采用最优/次优中继选择方案的安全中断概率均减小，这是由于增大 M，源节点采用 TAS 方案使得 $\mathrm{S}\to\mathrm{D}$ 链路平均 SNR 增大，从而增大了主信道容量，而窃听信道容量不变，MF 中继系统的安全容量增大，安全中断概率减小。当 $1/\alpha_k$ =30 dB，采用最优中继选择方案时，M=3 时的 MF 中继系统安全中断概率可由 M=1 时的 0.030 降为 0.005；采用次优中继选择方案时，M=3 时的 MF 中继系统安全中断概率可由 M=1 时的 0.066 降为 0.008。

合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的安全中断概率随 $\mathrm{R}\to\mathrm{D}$ 链路平均 SNR 的变化曲线如图 4 所示。$\mathrm{R}\to\mathrm{D}$ 链路平均 SNR 越高，MF 中继系统采用最优/次优中继选择的安全中断概率均越小。且在 K 相同的情况下，当 $1/\beta$ =0 和 $1/\beta\to\infty$ 时，两种中继选择方案下的 MF 系统的安全中断概率相同，这是由于 $1/\beta$ =0 时，D 接收到 R_k 的转发信息为 0，而 $\mathrm{S}\to\mathrm{D}$ 链路的 SNR 与中继节点无关，则最优/次优中继选择方案相同，所以采用两种中继选择方案的安全中断概率相同；而当 $1/\beta\to\infty$ 时，主信道 SNR 总为 $\mathrm{S}\to\mathrm{R}$ 链路的 SNR 值，所以采用两种中继选择方案的安全中断概率相同。

合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的遍历安全容量随 $\mathrm{S}\to\mathrm{D}$ 链路平均 SNR 的变化曲线如图 5 所示。

（1）$\mathrm{S}\to\mathrm{D}$ 链路平均 SNR 越高，MF 中继系

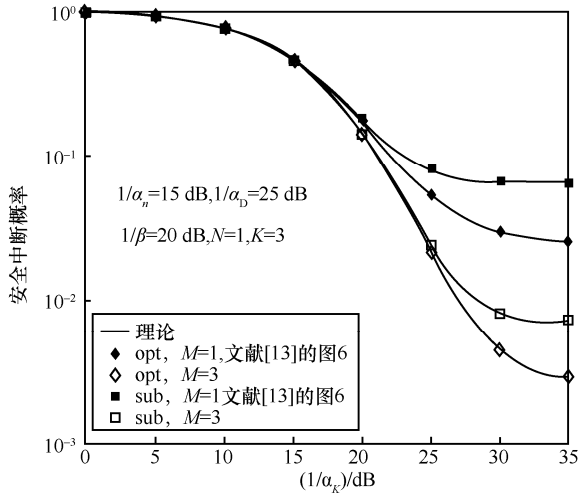

图 3　不同 $1/\alpha_k$ 下 MF 中继系统的安全中断概率

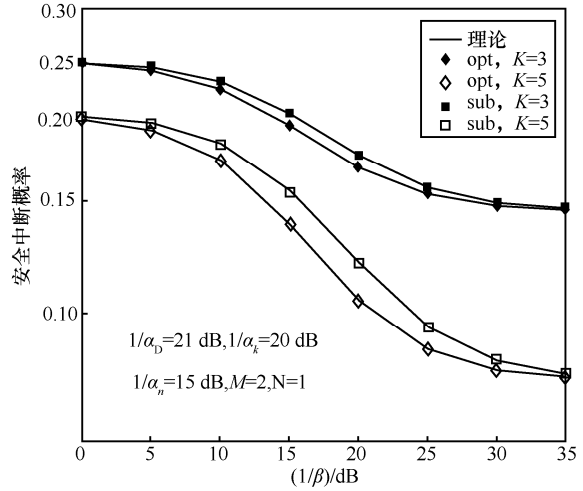

图 4　不同 $1/\beta$ 下 MF 中继系统的安全中断概率

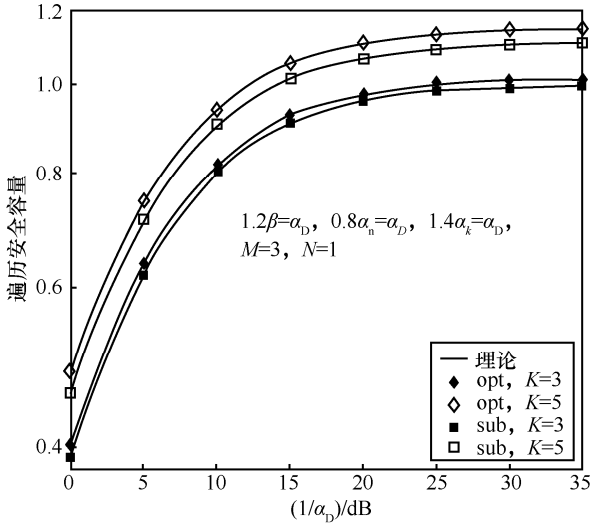

图 5　不同 $1/\alpha_D$、K 下 MF 中继系统的遍历安全容量

统采用最优/次优中继选择的遍历安全容量均越大，这是因为，基于图 4 的参数取值，$1/\alpha_k$、$1/\alpha_n$ 和 $1/\beta$ 均随 $1/\alpha_D$ 的增大而增大，且 $1/\alpha_k$ 和 $1/\beta$ 随 $1/\alpha_D$ 的变化均大于 $1/\alpha_n$ 的变化，所以当 $1/\alpha_D$ 较高时，主信道容量和窃听信道容量会随之增大，但是主信道容量的增加要大于窃听信道容量的增加，使得 MF 中继系统的遍历安全容量增加。

（2）增大中继节点的个数 K，MF 中继系统采用最优/次优中继选择的遍历安全容量均增大，这是由于增大 K 通过中继选择方案会增加主信道的容量，而窃听信道容量保持不变，使得 MF 中继系统的遍历安全容量增大。当 $1/\alpha_D$ =25 dB，采用最优中继选择方案时，K=5 相比于 K=3 时 MF 中继系统遍历安全容量增大约 0.137，采用次优中继选择方案时，K=5 相比于 K=3 时 MF 中继系统遍历安全容量增大约 0.116。

以不同源节点发射天线数 M 为参数的合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的遍历安全容量性能曲线如图 6 所示。MF 中继系统采用最优/次优中继选择方案的遍历安全容量均随源节点发射天线数 M 的增大而增大，这是由于增大 M，源节点采用 TAS 方案使得 $S\rightarrow D$ 链路 SNR 增大，从而增大了主信道容量，而窃听信道容量不变，使得 MF 中继系统的遍历安全容量增大。当 $1/\alpha_D$ =30 dB，采用最优中继选择方案时，M=3 相比于 M=1 时 MF 中继系统遍历安全容量增大约 0.114，采用次优中继选择方案时，M=3 相比于 M=1 时 MF 中继系统遍历安全容量增大约 0.175。

合谋窃听场景下源节点采用 TAS 的中继选择 MF 系统的遍历安全容量随 $S\rightarrow E$ 链路平均 SNR 的变化曲线如图 7 所示。

（1）$S\rightarrow E$ 链路平均 SNR 越高，MF 中继系统采用最优/次优中继选择的遍历安全容量均越小，这是由于，当 $1/\alpha_n$ 较大时，窃听信道容量增大，

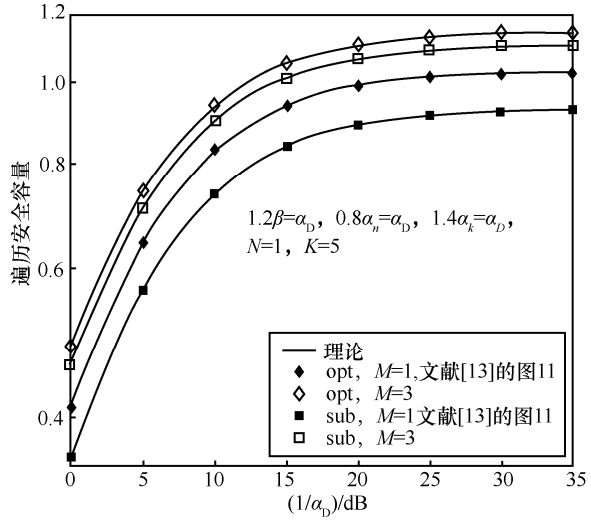

图 6　不同 $1/\alpha_{\mathrm{D}}$、M 下 MF 中继系统的遍历安全容量

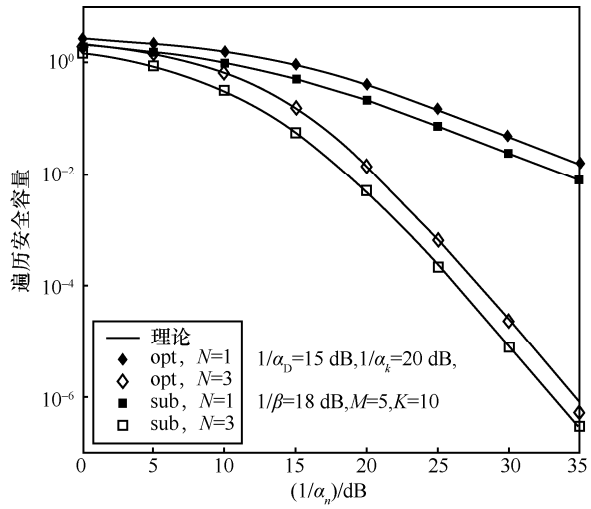

图 7　不同 $1/\alpha_n$ 下 MF 中继系统的遍历安全容量

而主信道容量保持不变，使得 MF 中继系统的安全容量减小，遍历安全容量减小。

（2）当 N 相同时，MF 中继系统采用最优中继选择方案的遍历安全容量总是大于采用次优中继选择方案的，这是由于最优中继选择方案选择使主信道 SNR 最大的中继转发信息，次优中继选择方案选择使 $\mathrm{S}\rightarrow\mathrm{R}$ 链路 SNR 最大的中继转发信息，因此其主信道 SNR 要小于最优中继选择方案下的主信道 SNR，而两种方案下的窃听信道容量相同，所以最优中继选择方案下的遍历安全容量大于次优中继选择方案的。

5　结束语

本文提出了合谋窃听者场景下源节点采用 TAS、中继节点采用最优/次优中继选择选择方案的 MF 系统，推导其安全中断概率、遍历安全容量的解析表达式，并通过 MATLAB 仿真实验加以验证。研究结果表明，源节点的发射天线数与中继节点数越多或者当窃听节点数越少时，MF 中继系统的物理层安全性能越好；在源节点的发射天线数、中继节点数、窃听节点数以及各链路平均 SNR 相同的条件下，MF 中继系统采用最优中继选择方案的遍历安全容量总是大于采用次优中继选择方案的。但是，本文仅研究了理想 CSI 下 MF 系统的安全性能，下一步将针对非理想 CSI 和信道估计下的 MF 系统的安全性能展开研究。

参考文献：

[1] WANG D, BAI B, ZHAO W B, et al. A survey of optimization approaches for wireless physical layer security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1878-1911.

[2] JU Y, WANG H Y, PEI Q Q, et al. Physical layer security in millimeter wave DF relay systems[J]. IEEE Transactions on Wireless Communications, 2019, 18(12): 5719-5733.

[3] 赵睿, 林鸿鑫, 贺玉成, 等. Nakagami 信道下 MIMO 解码转发中继系统的安全性能分析[J]. 电子与信息学报, 2016, 38(8): 1913-1919.
ZHAO R, LIN H X, HE Y C, et al. Secrecy performance analysis of MIMO decode-and-forward relay systems in Nakagami channels[J]. Journal of Electronics & Information Technology, 2016, 38(8): 1913-1919.

[4] 雷宏江, 张环, 刘俊杰, 等. 解码转发中继选择系统的安全性能分析[J]. 中国科学: 信息科学, 2017, 47(9): 1242-1254.
LEI H J, ZHANG H, LIU J J, et al. Security performance analysis of DF relay selection systems[J]. Scientia Sinica (Informationis), 2017, 47(9): 1242-1254.

[5] 冯友宏, 杨志, 丁绪星, 等. 无线协作网络中的最优中继选择方案及中断概率分析[J]. 电信科学, 2018, 34(11): 87-95.
FENG Y H, YANG Z, DING X X, et al. Optimal relay selection scheme and outage probability analysis in cooperative wireless networks[J]. Telecommunications Science, 2018, 34(11): 87-95.

[6] FENG Y H, YAN S H, YANG Z, et al. User and relay selection with artificial noise to enhance physical layer security[J]. IEEE Transactions on Vehicular Technology, 2018, 67(11):

10906-10920.

[7] 任婷洁, 李光球, 程英. 多中继与多用户选择的中继系统安全性能分析[J]. 电信科学, 2019, 35(8): 111-119.
REN T J, LI G Q, CHENG Y. Secure performance analysis of relay systems with multi-relay and multi-user selection[J]. Telecommunications Science, 2019, 35(8): 111-119.

[8] FARHAT J, BRANTE G, SOUZA R D. On the secure energy efficiency of TAS/MRC with relaying and jamming strategies[J]. IEEE Signal Processing Letters, 2017, 24(8): 1228-1232.

[9] DING Q F, LIU M X, DENG Y Q. Secrecy outage probability analysis for full-duplex relaying networks based on relay selection schemes[J]. IEEE Access, 2019(7): 105987-105995.

[10] CHEN X M, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security[J]. IEEE Communications Surveys & Tutorials, 2017, 19(2): 1027-1053.

[11] KIM S W. Modify-and-forward for securing cooperative relay communications[J]. arXiv: 1403.655, 2014.

[12] VIEN Q T, LE T A, NGUYEN H X, et al. A physical layer network coding based modify-and-forward with opportunistic secure cooperative transmission protocol[J]. Mobile Networks and Applications, 2019, 24(2): 464-479.

[13] CHU S I. Secrecy analysis of modify-and-forward relaying with relay selection[J]. IEEE Transactions on Vehicular Technology, 2019, 68(2): 1796-1809.

[14] JAKES W C. Microwave mobile communications[M]. Piscataway: IEEE Press, 1994.

[15] XIA J J, FAN L S, XU W, et al. Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers[J]. IEEE Transactions on Communications, 2019, 67(11): 7672-7685.

[16] PAPOULIS A, PILLAI S U. Probability, random variables, and stochastic processes, fourth edition[Z]. 2002.

[17] ZHAO R, TAN X, CHEN D H, et al. Secrecy performance of untrusted relay systems with a full-duplex jamming destination[J]. IEEE Transactions on Vehicular Technology, 2018, 67(12): 11511-11524.

[18] GRADSHTEYN I S, RYZHIK I M. Table of integrals, series, and products chapter 14-determinants[M]. Amsterdam: Elsevier, 1980: 1108-1113.

[作者简介]

程英（1995–），女，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。

李光球（1966– ），男，博士，杭州电子科技大学通信工程学院教授，主要研究方向为无线通信、信息论与编码等。

沈静洁（1996– ），女，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。

韦亮（1994– ），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。