第 46 卷 第 2 期 计 算 机 工 程 2020 年 2 月
Vol. 46 No. 2 Computer Engineering February 2020

·网络空间安全· 文章编号：1000-3428(2020)02-0148-06 文献标志码：A 中图分类号：TN929.5

广义空间调制系统的安全传输映射方案

陈发堂，陈嘉田，李 秀

（重庆邮电大学 通信与信息工程学院，重庆 400065）

摘 要：为提高时分双工无线通信系统中广义空间调制（GSM）的安全性，提出一种新的 GSM 安全传输映射方案。将合法信道状态信息引入映射过程中，分别重选由空间比特和星座比特映射的激活天线组合索引和星座符号索引，以增强 GSM 系统的安全性。仿真结果表明，该方案中的被动窃听者无法恢复激活天线组合索引与星座符号索引所携带的信息，其保密速率初始值较基于空间调制的方案提高 184.31%，增强了系统的安全性。

关键词：广义空间调制；映射方案；合法信道状态信息；保密速率；误比特率

开放科学（资源服务）标志码（OSID）：

中文引用格式：陈发堂，陈嘉田，李秀. 广义空间调制系统的安全传输映射方案[J]. 计算机工程，2020，46(2)：148-153.

英文引用格式：CHEN Fatang，CHEN Jiatian，LI Xiu. Mapping scheme of secure transmission for generalized spatial modulation system[J]. Computer Engineering，2020，46(2)：148-153.

Mapping Scheme of Secure Transmission for Generalized Spatial Modulation System

CHEN Fatang，CHEN Jiatian，LI Xiu

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

【Abstract】This paper proposes a new mapping scheme of secure transmission for Generalized Spatial Modulation (GSM) systems to improve GSM security in a time division duplex wireless communication system. The state information of legitimate channels is introduced into the mapping process. Then the active antenna combination index and constellation symbol index mapped by the space bit and the constellation bit are reselected to enhance system security. Simulation results show that the passive eavesdropper in this scheme is unable to recover the information carried by the active antenna combination index and the constellation symbol index. The initial value of the secrecy rate is increased by 184.31% compared with the scheme based on spatial modulation，demonstrating that the proposed scheme can enhance system security.

【Key words】Generalized Spatial Modulation (GSM)；mapping scheme；state information of legitimate channels；secrecy rate；Bit Error Rate (BER)

DOI：10.19678/j.issn.1000-3428.0054081

0 概述

空间调制（Spatial Modulation，SM）是一种空间复用多输入多输出（Multiple Input Multiple Output，MIMO）技术，其在每个时隙内只激活单根天线来传输单个星座符号。SM 通过将激活天线索引作为附加维度实现三维映射，以较低的硬件复杂度来实现较高的传输速率[1-3]，接收机通过检测激活天线索引获取空间域信息[4-5]。与传统的 MIMO 技术相比，空间调制解决了天线间同步和信道间干扰的问题[6]。为提升频谱效率，文献[7]提出在每个时隙内激活多根天线的广义空间调制（Generalized Spatial Modulation，GSM）技术，通过将激活天线组合索引作为空间维度，提升频谱效率，从而满足下一代大规模 MIMO 移动通信的高吞吐量要求。无线信道的广播特性使得信息传输覆盖区域内的所有用户都能接收到发送信号，导致机密信息易被恶意窃听者恢复窃取，因此，保证合法收发双方实现安全传输并使恶意窃听者无法窃取信息极为重要[8-9]。

文献[10]推导了空间调制与空移键控（Spatial Shift Keying，SSK）的保密速率，文献[11]给出 SSK

基金项目：国家科技重大专项（2017ZX03001021-004）；重庆教委科学技术研究项目（KJ1500428）。

作者简介：陈发堂（1965—），男，研究员，主研方向为通信安全、移动通信；陈嘉田、李 秀，硕士研究生。

收稿日期：2019-03-04 **修回日期：**2019-04-12 **E-mail：**chenjiatian94@163.com

和 SM 可实现保密速率的表达式,证明单天线传输的 SM 能够实现较高的保密速率。文献[12]在未知合法信道状态信息的情况下,将合法收发双方信道响应矩阵零空间的干扰和信号与星座符号进行组合,并作为发射机的发射信号,以增强安全传输性能,但该方案需要更多的发送天线,并需要合理分配信号与干扰的功率。文献[13]证明预编码辅助空间调制具有低概率拦截(Low Probability of Interception, LPI)特性,通过在发射机的预编码矩阵中加入随机分量来增强信息传输的安全性。文献[14-15]通过联合最小化窃听者接收功率和最大化合法接收者的接收功率,优化预编码器的预编码辅助空间调制,从而保证安全传输。文献[16]的发射机根据窃听者未知合法信道状态信息的瞬时模式,改变天线和星座符号索引的映射模式,以加强安全性。文献[17]的 SM 系统发射机利用合法信道状态信息选择一个已被固定规则重命名的激活天线来发送星座符号,但是该方案只对激活天线索引加密。文献[18]在空间调制系统中,利用合法信道状态信息旋转激活天线索引和星座符号索引进行安全传输。

目前,相关研究者人员大多关注空间调制和预编码辅助空间调制的安全传输,而针对 GSM 安全传输的研究较少。本文提出一种广义空间调制的安全传输映射方案,利用时分双工(Time Division Duplex, TDD)无线信道的互易性,根据合法信道状态信息重选激活天线组合索引与星座符号索引,增强广义空间调制系统的安全性。

1　系统模型

现有一个 MIMO 窃听系统,其包含发送者、合法接收者和被动窃听者,三者分别配置 N_{t}、N_{r} 和 N_{e} 根天线。由于在 TDD 模式下无线信道具有互易性,合法收发双方可通过发送导频序列获知射频链的合法信道状态信息,而被动窃听者无法获得。令 $\boldsymbol{H}_{\mathrm{R}}=[\boldsymbol{h}_{1,\mathrm{r}},\boldsymbol{h}_{2,\mathrm{r}},\cdots,\boldsymbol{h}_{k,\mathrm{r}},\cdots,\boldsymbol{h}_{N_{\mathrm{t}},\mathrm{r}}]$、$\boldsymbol{H}_{\mathrm{E}}=[\boldsymbol{h}_{1,\mathrm{e}},\boldsymbol{h}_{2,\mathrm{e}},\cdots,\boldsymbol{h}_{k,\mathrm{e}},\cdots,\boldsymbol{h}_{N_{\mathrm{e}},\mathrm{e}}]$ 分别为发送者与合法接收者、发送者与被动窃听者之间的快衰落和块不变信道冲激响应。其中,$\boldsymbol{h}_{k,\mathrm{r}}$和 $\boldsymbol{h}_{k,\mathrm{e}}$分别为 $\boldsymbol{H}_{\mathrm{R}}$ 和 $\boldsymbol{H}_{\mathrm{E}}$ 的第 k 列,$S=\{s_1,s_2,\cdots,s_M\}$ 为 M 阶调制星座符号集合。

GSM 系统在每一个时隙内激活 N_{a} 根发送天线,故从 N_{t} 根天线中选择 N_{a} 根的组合数为 $C_{N_{\mathrm{t}}}^{N_{\mathrm{a}}}$,有效使用的天线组合数为 $N=2^{\lfloor \mathrm{lb}(C_{N_{\mathrm{t}}}^{N_{\mathrm{a}}})\rfloor}$,其中$\lfloor\cdot\rfloor$表示向下取整。输入的信息被划分为长度为 $R_{\mathrm{GSM}}=R_{\mathrm{sym}}+R_{\mathrm{spa}}$ bit 的数据帧,其中,$R_{\mathrm{spa}}=\lfloor \mathrm{lb}\,N\rfloor$为空间比特,用于选择索引为 $k(1\leqslant k\leqslant N)$的激活发送天线组合 $I_k=\{i_1,i_2,\cdots,i_{N_{\mathrm{a}}}\}$,$R_{\mathrm{sym}}=\mathrm{lb}\,M$ 为星座比特数,用于选择星座符号索引 $l(1\leqslant l\leqslant M)$。

N_{a} 根天线对应索引 l 的发送星座符号向量为 $\boldsymbol{s}_l=[s_{i_1},s_{i_2},\cdots,s_{N_{\mathrm{a}}}]$,发送信号向量为 $\boldsymbol{x}=[\cdots,0,s_{i_1},\cdots,0,s_{i_2},\cdots,s_{i_{N_{\mathrm{a}}}},0,\cdots]^{\mathrm{T}}\in\mathbb{C}^{N_{\mathrm{t}}\times 1}$,其中,$N_{\mathrm{a}}$ 个元素非零,其余元素全为零。系统的频谱效率为 R_{GSM} bit/s/Hz,合法接收者与被动窃听者的接收信号向量 $\boldsymbol{y}_{\mathrm{r}}\in\mathbb{C}^{N_{\mathrm{r}}\times 1}$,$\boldsymbol{y}_{\mathrm{e}}\in\mathbb{C}^{N_{\mathrm{e}}\times 1}$可表示为如下形式:

$$\boldsymbol{y}_{\mathrm{r}}=\boldsymbol{H}_{\mathrm{R}}x+\boldsymbol{\varepsilon}_{\mathrm{r}}=\sum_{k'=i_1}^{i_{N_{\mathrm{a}}}}\boldsymbol{h}_{k',\mathrm{r}}x_k'+\boldsymbol{\varepsilon}_{\mathrm{r}}=\boldsymbol{H}_{I_k,\mathrm{R}}\boldsymbol{s}_l+\boldsymbol{\varepsilon}_{\mathrm{r}}\tag{1}$$

$$\boldsymbol{y}_{\mathrm{e}}=\boldsymbol{H}_{\mathrm{E}}x+\boldsymbol{\varepsilon}_{\mathrm{e}}=\sum_{k'=i_1}^{i_{N_{\mathrm{a}}}}\boldsymbol{h}_{k',\mathrm{e}}x_k'+\boldsymbol{\varepsilon}_{\mathrm{e}}=\boldsymbol{H}_{I_k,\mathrm{E}}\boldsymbol{s}_l+\boldsymbol{\varepsilon}_{\mathrm{e}}\tag{2}$$

其中,$k'\in I_k$,x_k'为 x 的第 k'个元素,$\boldsymbol{\varepsilon}_{\mathrm{r}}\in\mathbb{C}^{N_{\mathrm{r}}\times 1}$与 $\boldsymbol{\varepsilon}_{\mathrm{e}}\in\mathbb{C}^{N_{\mathrm{e}}\times 1}$是协方差矩阵为 $\sigma_{\mathrm{r}}^2\boldsymbol{E}_{N_{\mathrm{r}}}$和 $\sigma_{\mathrm{e}}^2\boldsymbol{E}_{N_{\mathrm{e}}}$的复加性高斯白噪声(Additive White Gaussian Noise, AWGN)。$\boldsymbol{H}_{I_k,\mathrm{R}}=[\boldsymbol{h}_{i_1,\mathrm{r}},\boldsymbol{h}_{i_2,\mathrm{r}},\cdots,\boldsymbol{h}_{i_{N_{\mathrm{a}}},\mathrm{r}}]$为激活天线组合 I_k 对应于 $\boldsymbol{H}_{\mathrm{R}}$ 的子矩阵,$\boldsymbol{H}_{I_k,\mathrm{E}}=[\boldsymbol{h}_{i_1,\mathrm{e}},\boldsymbol{h}_{i_2,\mathrm{e}},\cdots,\boldsymbol{h}_{i_{N_{\mathrm{a}}},\mathrm{e}}]$为激活天线组合 I_k 对应于 $\boldsymbol{H}_{\mathrm{E}}$ 的子矩阵。合法接收者与被动窃听者采用最大似然(Maximum Likelihood, ML)检测,具体过程如下:

$$(\hat{k},\hat{l})=\underset{k\in P,l\in Q}{\operatorname{argmin}}\|\boldsymbol{y}_{\mathrm{r}}-\boldsymbol{H}_{I_k,\mathrm{R}}\boldsymbol{s}_l\|_{\mathrm{F}}^2\tag{3}$$

$$(\hat{k}_{\mathrm{e}},\hat{l}_{\mathrm{e}})=\underset{k_{\mathrm{e}}\in P,l_{\mathrm{e}}\in Q}{\operatorname{argmin}}\|\boldsymbol{y}_{\mathrm{e}}-\boldsymbol{H}_{I_{k_{\mathrm{e}}},\mathrm{E}}\boldsymbol{s}_{l_{\mathrm{e}}}\|_{\mathrm{F}}^2\tag{4}$$

其中,$P=\{1,2,\cdots,N\}$,$Q=\{1,2,\cdots,M\}$。

2　本文映射方案

本文方案利用窃听者未知的合法信道状态信息,重选由空间比特与星座比特映射得到的天线组合索引与星座符号索引,实现 GSM 系统的安全传输,如图 1 所示。下文分别从发送者、合法接收者和被动窃听者 3 个方面进行阐述。

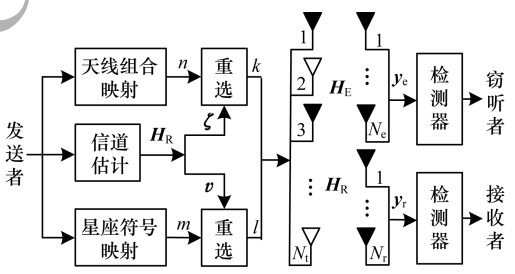

图 1　本文方案的系统框图

Fig. 1　System block diagram of the proposed scheme

2.1　发送者

发送者按照以下步骤进行处理:

步骤 1　计算 N 个候选天线组合对应的合法信道矩阵$\|\boldsymbol{H}_{I_1,\mathrm{R}}\|_{\mathrm{F}}^2,\cdots,\|\boldsymbol{H}_{I_k,\mathrm{R}}\|_{\mathrm{F}}^2,\cdots,\|\boldsymbol{H}_{I_N,\mathrm{R}}\|_{\mathrm{F}}^2$,将这 N 个值升序排序构造向量 $\boldsymbol{\zeta}$,如式(5)所示。

$$\boldsymbol{\zeta}=[\zeta_1,\zeta_2,\cdots,\zeta_n,\cdots,\zeta_N]\tag{5}$$

其中,$\zeta_n=\|\boldsymbol{H}_{I_k,\mathrm{R}}\|_{\mathrm{F}}^2$。

步骤 2　传统的 GSM 系统发送端在每一个时隙内的空间比特 $n_{\mathrm{bit}}=b_ub_{u-1}\cdots b_2b_1$,$u=\mathrm{lb}\,N$,可映射索引 n 的激活天线组合 I_n。

步骤 3 将原始天线组合索引 n 按如下规则进行重选,得到发送端的激活天线组合 $I_k(1\leqslant k\leqslant N)$。

$$n_{\text{bit}}\rightarrow n\rightarrow\zeta_n\rightarrow\|\boldsymbol{H}_{I_k,\text{R}}\|_{\text{F}}^2\rightarrow I_k \tag{6}$$

步骤 4 将步骤 1 中的前 M 个候选天线组合对应的合法信道矩阵进行升序排列,构建星座符号索引重选向量 $\boldsymbol{v}$,其中,$v_m=\|\boldsymbol{H}_{I_l,\text{R}}\|_{\text{F}}^2$。

$$\boldsymbol{v}=[v_1,v_2,\cdots,v_m,\cdots,v_M] \tag{7}$$

步骤 5 传统的 GSM 系统发送端的星座比特为 $m_{\text{bit}}=b_vb_{v-1}\cdots b_2b_1$,$v=\text{lb}\,M$,其对应的星座符号索引为 m。

步骤 6 将原始星座符号索引 m 按如下规则进行重选,得到发送端的星座符号索引 $l(1\leqslant l\leqslant M)$。

$$m_{\text{bit}}\rightarrow m\rightarrow\boldsymbol{v}_m\rightarrow\|\boldsymbol{H}_{I_l,\text{R}}\|_{\text{F}}^2\rightarrow l \tag{8}$$

步骤 7 由星座符号索引 l 可得星座符号 s_l、星座符号向量 $\boldsymbol{s}_l$ 和发送信号向量 $\boldsymbol{x}$,发送端使用激活的天线组合 I_k。

2.2 合法接收者

合法接收者得到 y_{r} 后,由时分双工无线信道的互易性可以得到 $\boldsymbol{H}_{\text{R}}$,并执行下面步骤:

步骤 1 利用式(3)进行最大似然检测,得到 $\hat{k}$ 和 $\hat{l}$。

步骤 2 根据式(5)构造向量 $\boldsymbol{\zeta}$,通过式(6)的发送端天线组合映射进行逆过程解析,得到空间比特 $\hat{n}_{\text{bit}}$。

$$I_k\rightarrow\|\boldsymbol{H}_{\hat{k},\text{R}}\|_{\text{F}}^2\rightarrow\zeta_{\hat{n}}\rightarrow\hat{n}\rightarrow\hat{n}_{\text{bit}} \tag{9}$$

步骤 3 根据式(7)构造向量 $\boldsymbol{v}$,由式(8)的发送端星座符号映射进行逆过程解析,得到星座比特 $\hat{m}_{\text{bit}}$。

$$\hat{l}\rightarrow\|\boldsymbol{H}_{I_{\hat{l}},\text{R}}\|_{\text{F}}^2\rightarrow\zeta_{\hat{m}}\rightarrow\hat{m}\rightarrow\hat{m}_{\text{bit}} \tag{10}$$

2.3 被动窃听者

由于空间具有去相关特性,如果被动窃听者与发送者、合法接收者的距离超过半波长,则其无法得到 $\boldsymbol{H}_{\text{R}}$[14,17],因此窃听者无法由式(5)、式(7)构造向量 $\boldsymbol{\zeta}$、$\boldsymbol{v}$,只能按以下步骤进行处理:

步骤 1 根据式(4)执行最大似然检测,得到 $\hat{k}_{\text{e}}$ 和 $\hat{l}_{\text{e}}$。

步骤 2 被动窃听者与发送者之间的信道矩阵 $\boldsymbol{H}_{\text{E}}$ 与 $\boldsymbol{H}_{\text{R}}$ 不同,故其在式(9)、式(10)的逆映射过程中不能实现 $I_{\hat{k}_{\text{e}}}\rightarrow\|\boldsymbol{H}_{\hat{k}_{\text{e}},\text{R}}\|_{\text{F}}^2$,$\hat{l}_{\text{e}}\rightarrow\|\boldsymbol{H}_{I_{\hat{l}_{\text{e}}},\text{R}}\|_{\text{F}}^2$,只能进行如下过程:

$$I_{\hat{k}_{\text{e}}}\rightarrow\tilde{n}_{\text{e}}\rightarrow\tilde{n}_{\text{bit,e}} \tag{11}$$

$$\hat{l}_{\text{e}}\rightarrow\tilde{m}_{\text{e}}\rightarrow\tilde{m}_{\text{bit,e}} \tag{12}$$

其中,$\tilde{n}_{\text{e}}$ 与 $\tilde{m}_{\text{e}}$ 通过随机取值来尝试实现发送者映射的逆过程,从而恢复空间比特与星座比特,并使 $P(\tilde{n}_{\text{e}}=n)=\dfrac{1}{N}$,$P(\tilde{m}_{\text{e}}=m)=\dfrac{1}{M}$。

3 保密速率分析

基于信息论知识,本文方案的保密速率可通过合法接收者信息量减去被动窃听者的信息量得到。根据式(3),$\boldsymbol{y}_{\text{r}}$ 的条件概率密度函数如下:

$$P(\boldsymbol{y}_{\text{r}}\mid\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)=\frac{1}{(\pi\sigma_{\text{r}}^2)^{N_{\text{r}}}}\exp\left(-\frac{\|\boldsymbol{y}_{\text{r}}-\boldsymbol{H}_{I_n,\text{R}}\boldsymbol{s}_m\|^2}{\sigma_{\text{r}}^2}\right) \tag{13}$$

由于 n 与 m 皆为均匀分布,因此 $\boldsymbol{y}_{\text{r}}$ 的概率分布函数如下:

$$P(\boldsymbol{y}_{\text{r}})=\frac{1}{NM}\sum_{n=1}^{N}\sum_{m=1}^{M}\left[\frac{1}{(\pi\sigma_{\text{r}}^2)^{N_{\text{r}}}}\exp\left(-\frac{\|\boldsymbol{y}_{\text{r}}-\boldsymbol{H}_{I_n,\text{R}}\boldsymbol{s}_m\|^2}{\sigma_{\text{r}}^2}\right)\right] \tag{14}$$

故合法接收者的互信息如式(15)所示。

$$\begin{aligned}I(\boldsymbol{y}_{\text{r}};\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)=&\int\sum_{n=1}^{N}\sum_{m=1}^{M}P(\boldsymbol{y}_{\text{r}},\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)\times\\&\text{lb}\,\frac{P(\boldsymbol{y}_{\text{r}},\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)}{P(\boldsymbol{y}_{\text{r}})P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)}\text{d}_{y_{\text{r}}}=\\&\frac{1}{MN}\sum_{n=1}^{N}\sum_{m=1}^{M}\int P(\boldsymbol{y}_{\text{r}}\mid\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)\times\\&\text{lb}\,\frac{P(\boldsymbol{y}_{\text{r}}\mid\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)}{\frac{1}{MN}\sum_{n_1=1}^{N}\sum_{m_1=1}^{M}P(\boldsymbol{y}_{\text{r}}\mid\boldsymbol{H}_{I_{n_1},\text{R}},\boldsymbol{s}_{m_1})}\text{d}_{y_r}=\\&\text{lb}\,MN-\frac{1}{MN}\sum_{n=1}^{N}\sum_{m=1}^{M}\int P(\boldsymbol{y}_{\text{r}}\mid\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)\times\\&\text{lb}\left\{\sum_{n_1=1}^{N}\sum_{m_1=1}^{M}\exp\left(-\frac{\|\boldsymbol{y}_{\text{r}}-\boldsymbol{H}_{I_{n_1},\text{R}},\boldsymbol{s}_{m_1}\|^2-\|\boldsymbol{y}_{\text{r}}-\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m\|^2}{\sigma_{\text{r}}^2}\right)\right\}\text{d}_{y_{\text{r}}}\end{aligned} \tag{15}$$

令 $d_{n,m}^{n_1,m_1}=\boldsymbol{H}_{I_n,\text{R}}\boldsymbol{s}_m-\boldsymbol{H}_{I_{n_1},\text{R}}\boldsymbol{s}_{m_1}$,则式(15)可写为如下形式:

$$\text{lb}\,MN-\frac{1}{MN}\sum_{n=1}^{N}\sum_{m=1}^{M}E\boldsymbol{\varepsilon}_{\text{r}}\cdot\text{lb}\left\{\sum_{n_1=1}^{N}\sum_{m_1=1}^{M}\exp\left(-\frac{\|d_{n,m}^{n_1,m_1}+\boldsymbol{\varepsilon}_{\text{r}}\|^2-\|\boldsymbol{\varepsilon}_{\text{r}}\|^2}{\sigma_{\text{r}}^2}\right)\right\} \tag{16}$$

如第 2 节所述,被动窃听者无法获知 $\boldsymbol{H}_{\text{R}}$,并且无线信道的差异性导致 $\boldsymbol{H}_{\text{E}}$ 与 $\boldsymbol{H}_{\text{R}}$ 不同,故窃听者无法根据 $\boldsymbol{H}_{\text{E}}$ 计算出 $\boldsymbol{\zeta}$ 和 $\boldsymbol{v}$ 及其发送端映射重选的逆过程。

由 $P(\boldsymbol{H}_{I_{\tilde{n}_{\text{e}},\text{R}}}=\boldsymbol{H}_{I_n,\text{R}}\mid\hat{k}_{\text{e}})=P(\boldsymbol{H}_{I_n,\text{R}})=\dfrac{1}{N}$ 和 $P(\boldsymbol{s}_{\tilde{m}_{\text{e}}}=\boldsymbol{s}_m\mid\hat{l}_{\text{e}})=P(\boldsymbol{s}_m)=\dfrac{1}{M}$ 可得如下公式:

$$P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m\mid\boldsymbol{y}_{\text{e}})=P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m\mid\hat{k}_{\text{e}},\hat{l}_{\text{e}})=P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m) \tag{17}$$

在式(17)两边同时乘以 $P(\boldsymbol{y}_{\text{e}})$ 可得:

$$P(\boldsymbol{y}_{\text{e}},\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)=P(\boldsymbol{y}_{\text{e}})P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m) \tag{18}$$

由此可得被动窃听者的互信息,如式(19)所示。

$$I(\boldsymbol{y}_{\text{e}};\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)=\int\sum_{n=1}^{N}\sum_{m=1}^{M}P(\boldsymbol{y}_{\text{e}},\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)\times\text{lb}\,\frac{P(\boldsymbol{y}_{\text{e}},\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)}{P(\boldsymbol{y}_{\text{e}})P(\boldsymbol{H}_{I_n,\text{R}},\boldsymbol{s}_m)}=0 \tag{19}$$

根据式(16)、式(19)可得本文方案的保密速率,如式(20)所示。

$$R_s = \max\{0, I(\boldsymbol{y}_r;\boldsymbol{H}_{I_n,R},\boldsymbol{s}_m) - I(\boldsymbol{y}_e;\boldsymbol{H}_{I_n,R},\boldsymbol{s}_m)\} = \max\{0, I(\boldsymbol{y}_r;\boldsymbol{H}_{I_n,R},\boldsymbol{s}_m)\} \quad (20)$$

式(19)表明即使被动窃听者正确检测 $\hat{k}_e$ 与 $\hat{l}_e$,也无法恢复发送端发送的空间比特与星座比特,其互信息量为 0,只能随机确定每一个二进制比特,故被动窃听者的误比特率(Bit Error Rate, BER)为 50%[18]。由式(20)可知,本文方案的保密速率取值完全由合法接收者的互信息量决定,而与被动窃听者无关。

4　仿真结果与分析

4.1　仿真结果

本文对第 2 节提出的广义空间调制系统安全传输的映射方案进行蒙特卡罗仿真,并根据式(20)计算出系统的保密速率,然后将该映射方案与文献[18]中基于空间调制的安全传输方案进行对比。为保证激活天线的稀疏性,令 $N_a = 2$,参数配置如表 1所示[19]。图 2 给出保密速率在不同 M 下随信噪比(Signal-Noise Ratio, SNR)变化的曲线。

表 1　仿真参数配置

Table 1　Configuration of simulation parameters

序号	N_t	N_a	N	M	N_r	N_e
1	4	2	4	2	4	4
2	8	2	16	2	4	4
3	8	2	16	4	4	4
4	16	2	64	4	4	4
5	32	2	256	4	4	4

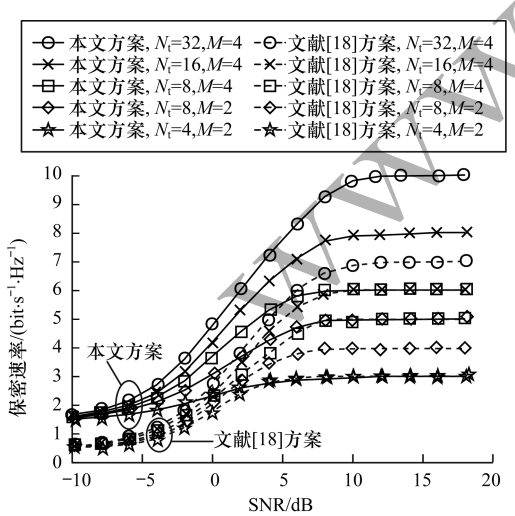

图 2　保密速率在不同 M 下随 SNR 变化的曲线

Fig. 2　Curve of the privacy rate with SNR under different values of M

由图 2 可以看出,随着发射 SNR 的增加,衰落信道中的保密速率逐渐上升并趋于稳定。在相同的仿真参配置下,本文方案的系统保密速率初始值比文献[18]方案提高 184.31%。这是因为在低信噪比区域,广义空间调制具有分集增益优势,所以其保密速率要大于文献[18]方案。当 SNR 达到 12 dB 时,保密速率达到上限值,即 $R_{GSM} = \text{lb}\, MN$ bit/s/Hz。在保证激活天线稀疏性的前提下(即 N 大于文献[18]方案的发机天线数),本文方案能够达到更高的保密速率。

为了验证本文方案的优越性,在 $N_t = 8$, $N_r = 4$ 和 QPSK 配置下分别计算本文方案、文献[15]方案、文献[17]方案和文献[18]方案的保密速率,如图 3 所示。由于文献[15]方案基于预编码空间调制系统,其保密速率与合法接收者天线数 N_r 有关,当窃听者天线数目 $N_e \leqslant N_t - N_r$ 且以整体功率分配因子 θ 最优为前提时,保密速率能够达到理论上限,故本文分别给出 $N_e = 4$ 和 $N_e = 2$ 两种配置下的保密速率。而文献[17]方案与文献[18]方案针对提升空间调制系统的保密速率,其主要受发送者天线数 N_t 与星座符号的调制阶数 M 影响,故 $N_e \equiv 4$。由图 3 可知,本文方案的保密速率最高可达 6 bit/s/Hz,且总是高于其他 3 种方案。文献[17]方案和文献[18]方案的保密速率最高分别可达 3 bit/s/Hz 和 5 bit/s/Hz。而文献[15]方案的保密速率最高可达 4 bit/s/Hz,其性能低于文献[18]方案且高于文献[17]方案,在低 SNR 区域且 N_e 较小时,文献[15]方案的保密速率随 SNR 的提升速率较快。由于文献[15]方案与文献[17]方案的保密速率均低于本文方案与文献[18]方案,因此下文主要对比文献[18]方案与本文方案。

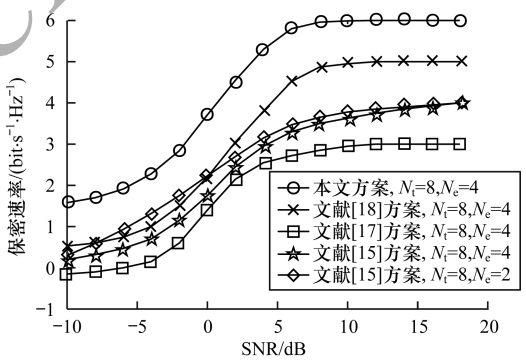

图 3　4 种方案的保密速率对比

Fig. 3　Comparison of secrecy rates between 4 schemes

图 4 为合法接收者和被动窃听者在表 1 参数配置下的 BER 曲线。可以看出,窃听者误比特率在任意信噪比下都为 0.5,与第 3 节的分析一致,窃听者无法恢复空间比特与信息比特,而合法接收者的 BER 比窃听者低得多,表明本文方案能够实现安全传输。此外,采用式(1)的 ML 检测时,接收者的 BER 受到天线组合与星座符号的联合搜索空间的影响,即联合搜索空间越大,BER 性能越差。

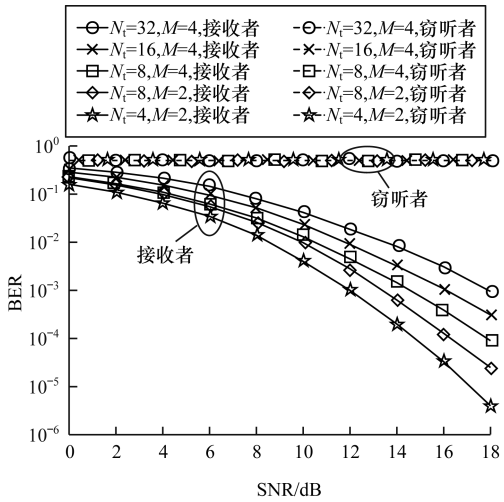

图 4 合法接收者与被动窃听者的 BER 曲线

Fig. 4 BER curve of legitimate receiver and passive eavesdropper

图 5 给出在 $N_t=8$、$N_a=2$、$N_r=N_e=4$ 和 QPSKS 情况下,被动窃听者与合法接收者信道相关时的 BER 性能。$\boldsymbol{H}_E=\delta\boldsymbol{H}_R+(1-\delta)\boldsymbol{H}_{ICR}$ 为构建的信道相关模型,δ 为相关因子,$\boldsymbol{H}_{ICR}$ 为独立信道矩阵。当相关因子 δ 增大时,窃听者的 BER 随信噪比的增大而降低,在信噪比为 15 dB 左右时,BER 趋于稳定,表明本文方案能够有效降低窃听者与合法收发信道的相关性。信道估计误差和 $(1-\delta)\boldsymbol{H}_{ICR}$ 项是窃听者 BER 存在上界的主要原因[20]。

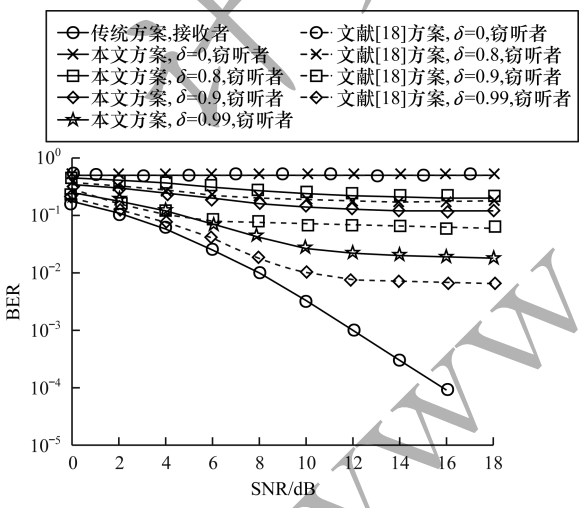

图 5 不同 δ 下被动窃听者和合法接收者的 BER 对比

Fig. 5 Comparison of BER between passive eavesdropper and legitimate receiver under different related factors

4.2 复杂度分析

与传统映射方案相比,本文方案复杂度的增加主要集中在天线组合索引与星座符号索引的重选上,即构造向量 $\boldsymbol{\zeta}$、$\boldsymbol{v}$ 的过程。计算 N 组候选天线组合的 $\|\boldsymbol{H}_{I_k,R}\|_F^2$ 复杂度为 $(4N_rN_a-1)\times N$,生成向量 $\boldsymbol{\zeta}$ 的过程中进行升序排序时需要比较 $N-1$ 次,故重选天线组合的复杂度为 $4NN_rN_a-1$。生成向量 $\boldsymbol{v}$ 无需计算 $\|\boldsymbol{H}_{I_k,R}\|_F^2$,取 N 个值的前 M 项进行升序排列需要比较 $M-1$ 次,故重选星座符号复杂度为 $M-1$,本文映射方案的总复杂度为 $4NN_rN_a+M-2$。

文献[18]方案的复杂度为 N_t+M-2,这是因为其只对生成的重选向量进行排序,未将向量各元素的计算过程考虑在内,故本文方案的复杂度比文献[18]方案高。此外,文献[18]方案在对天线和星座符号重选时生成固定数量的向量元素,而本文方案受候选天线集合数目的影响,可对稀疏性与复杂度进行权衡,通过不同激活天线数 N_a 改变候选天线集合数目。由仿真结果可知,本文方案的保密速率和抗信道相关性更高,尤其在对安全传输要求较高的通信场景,本文方案能实现更可靠的信息传输。

5 结束语

本文提出一种广义空间调制系统的安全传输映射方案,并从发送者、合法接收者和被动窃听者 3 个角度进行阐述。根据信息论知识推导保密速率公式并分析被动窃听者的 BER 性能。理论分析与仿真结果表明,与文献[18]中基于空间调制的安全传输方案相比,该方案以计算复杂度为代价,可实现更高的保密速率和频谱效率以及更低的误比特率,验证了该方案能够有效抵消信道相关的影响,增强广义空间调制的传输安全性。然而,本文主要基于收发双方已知合法信道状态信息对广义空间调制系统的映射方案进行设计,考虑到实际无线信道历经各类衰落,收发双方只能获得不完全合法的信道状态信息。因此,下一步需在不完全信道状态信息的情况下,对本文方案进行优化,以改善其安全性。

参考文献

[1] MESLEH R Y, HAAS H, SINANOVIC S, et al. Spatial modulation [J]. IEEE Transactions on Vehicular Technology, 2008, 57(4): 2228-2241.

[2] JEGANATHAN J, GHRAYEB A, SZCZECINSKI L. Spatial modulation: optimal detection and performance analysis [J]. IEEE Communications Letters, 2008, 12(8): 545-547.

[3] CHEN Fatang, ZHANG Dingquan, YI Rui. Iterative detection algorithm under superposition coded for generalized space modulation system [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2018, 30(2): 42-48. (in Chinese)
陈发堂,张丁全,易润. 广义空间调制系统分层叠加编码的迭代检测[J]. 重庆邮电大学学报(自然科学版), 2018, 30(2): 42-48.

[4] ALSHAMALI A, QUZA B. Spatial modulation: performance evaluation in Nakagami fading channels[C]//Proceedings of the 5th IEEE GCC Conference and Exhibition. Washington D.C., USA: IEEE Press, 2009: 1-4.

[5] CHEN Fatang, LI Yuhe, LIU Yan. Low-complexity signal detection algorithm based on GPSM[J]. Study on Optical Communications, 2017, 43(5): 61-64. (in Chinese)
陈发堂,李玉河,刘燕. 基于广义预编码辅助空间调制的分组检测算法[J]. 光通信研究,2017,43(5):61-64.

[6] DI RENZO M, HAAS H, GHRAYEB A, et al. Spatial modulation for generalized MIMO: challenges, opportunities, and implementation[J]. Proceedings of the IEEE, 2014, 102(1): 56-103.

[7] YOUNIS A, SERAFIMOVSKI N, MESLEH R, et al. Generalized spatial modulation [C]//Proceedings of IEEE Conference Record of the 44th Asilomar Conference on Signals, Systems and Computers. Washington D. C., USA: IEEE Press, 2010: 1498-1502.

[8] REN Pinyi, TANG Xiao. A review on physical layer security techniques for 5G wireless networks[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(5): 69-77. (in Chinese)
任品毅,唐晓. 面向 5G 的物理层安全技术综述[J]. 北京邮电大学学报,2018,41(5):69-77.

[9] ZHU Jiang, WANG Yan, YANG Tian. Secure transmission mechanism based on time reversal over wireless multipath channels[J]. Acta Physica Sinica, 2018, 67(5): 7-17. (in Chinese)
朱江,王雁,杨甜. 无线多径信道中基于时间反演的物理层安全传输机制[J]. 物理学报,2018,67(5):7-17.

[10] AGHDAM S R, DUMAN T M, DI RENZO M. On secrecy rate analysis of spatial modulation and space shift keying[C]// Proceedings of IEEE International Black Sea Conference on Communications and Networking. Washington D. C., USA: IEEE Press, 2015: 63-67.

[11] GUAN Xinrong, CAI Yueming, YANG Weiwei. On the secrecy mutual information of spatial modulation with finite alphabet[C]//Proceedings of International Conference on Wireless Communications and Signal Processing. Washington D. C., USA: IEEE Press, 2012: 1-4.

[12] WANG L, BASHAR S, WEI Y, et al. Secrecy enhancement analysis against unknown eavesdropping in spatial modulation[J]. IEEE Communications Letters, 2015, 19(8): 1351-1354.

[13] WU Feilong, DONG Chen, YANG Lieliang, et al. Secure wireless transmission based on precoding-aided spatial modulation [C]//Proceedings of IEEE Global Communications Conference. Washington D. C., USA: IEEE Press, 2015: 1-6.

[14] WU Feilong, ZHANG Rong, YANG Lieliang, et al. Transmitter precoding aided spatial modulation for secrecy communications [J]. IEEE Transactions on Vehicular Technology, 2016, 65(1): 467-471.

[15] WU Feilong, YANG Lieliang, WANG Wenjie, et al. Secret precoding-aided spatial modulation [J]. IEEE Communications Letters, 2015, 19(9): 1544-1547.

[16] YANG Y, GUIZANI M. Mapping-varied spatial modulation for physical layer security: transmission strategy and secrecy rate[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 877-889.

[17] WANG Xin, WANG Xia, SUN Li. Spatial modulation aided physical layer security enhancement for fading wiretap channels [C]//Proceedings of the 8th International Conference on Wireless Communications and Signal Processing. Washington D. C., USA: IEEE Press, 2016: 1-5.

[18] JIANG Xueqin, WEN Miaowen, HAI Han, et al. Secrecy-enhancing scheme for spatial modulation[J]. IEEE Communications Letters, 2018, 22(3): 550-553.

[19] LIU Jianling, CHEN Zhigang, WANG Lei. An adaptive modulation algorithm with low complexity for generalized spatial modulation[J]. Journal of Xi'an Jiaotong University, 2016, 50(4): 48-53, 67. (in Chinese)
刘健伶,陈志刚,王磊. 一种自适应广义空间调制及其低复杂度算法[J]. 西安交通大学学报,2016,50(4):48-53,67.

[20] ANNAVAJJALA R, COSMAN P C, MILSTEIN L B. Performance analysis of linear modulation schemes with generalized diversity combining on rayleigh fading channels with noisy channel estimates[J]. IEEE Transactions on Information Theory, 2007, 53(12): 4701-4727.

编辑　樊丽娜