星地异构共生安全保密性能分析

赵璇[1]，尹志胜[2, 3]，承楠[2, 3]，刘永红[1]，王兆薇[2]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710126；2. 西安电子科技大学通信工程学院，陕西 西安 710071；
3. 空天地一体化综合业务网全国重点实验室，陕西 西安 710071）

摘　要：星地融合网络中，卫星与地面异构网络采用频谱共享技术可以提升系统资源利用率。然而，这导致卫星与地面异构通信链路之间互相受到同频干扰，恶化了通信性能。星地异构共生安全通信可以将不利于通信的干扰变废为宝，使星地异构链路的安全传输形成互惠共生关系。对于窃听威胁场景下的星地安全传输需求，理论分析了星地共生安全通信的保密速率和保密中断概率，给出了保密速率的理论下界，且仿真结果验证了理论分析的正确性。研究结果表明，无需消耗额外资源，卫星和地面链路能够利用互惠干扰以共生的形式分别实现安全传输。

关键词：星地异构融合网络；共生安全；安全传输；保密性能分析
中图分类号：TN915.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00456

Secrecy performance analysis of satellite-terrestrial heterogeneous symbiotic security

ZHAO Xuan[1], YIN Zhisheng[2, 3], CHENG Nan[2, 3], LIU Yonghong[1], WANG Zhaowei[2]
1. School of Cyber Engineering, Xidian University, Xi'an 710126, China
2. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China
3. State Key Laboratory of Integrated Services Networks, Xi'an 710071, China

Abstract: In integrated satellite-terrestrial networks, satellite and terrestrial heterogeneous networks employ spectrum sharing technology to enhance system resource utilization. However, this approach results in mutual co-frequency interference between satellite and terrestrial communication links, degrading overall communication performance. The concept of satellite-terrestrial heterogeneous symbiotic secure communication is proposed to convert detrimental interference into a beneficial resource, making the safe transmission of satellite-terrestrial heterogeneous links form a mutually beneficial symbiotic relationship. The need for secure satellite-terrestrial transmission under eavesdropping threats was addressed by theoretically analyzing the secrecy rate and secrecy outage probability of the symbiotic secure communication system. A theoretical lower bound for the secrecy rate was derived, and simulation results validated the theoretical analysis. The findings indicate that the satellite and terrestrial links can be leveraged to achieve secure transmission through reciprocal interference, without the need for additional resource allocation.

Key words: satellite-terrestrial heterogeneous network, symbiotic security, secure transmission, secrecy performance analysis

0　引言

卫星通信作为无线通信技术的重要应用形式，因为广域覆盖能力和广播特性，已成为构建全球通信网络的重要支撑，为解决地面网络覆盖不足和提升通信网络可靠性发挥了关键作用。然而，这些优

收稿日期：2024−11−06；**修回日期：**2024−12−09
通信作者：尹志胜，zsyin@xidian.edu.cn
基金项目：国家自然科学基金资助项目（No. 62201432，No. 62101429）
Foundation Items: The National Natural Science Foundation of China (No. 62201432, No. 62101429)

势也使卫星通信面临着严重的无线通信安全问题[1]。由于无线通信的开放性，广播信号易被截获，如果缺乏有效的加密保护，则非授权用户可以轻易窃听通信内容，从而威胁信息的保密性和完整性[2]。尤其在卫星通信中，窃听者（Eves, eavesdroppers）可能分布在广泛的地理区域内，这使得传统的安全措施难以有效地应对[3-5]。

为了应对这些安全威胁，物理层安全（PLS, physical layer security）作为一种有效的安全手段，在传统无线通信领域中得到了广泛的研究和应用。作为上层密码学协议的补充，PLS 技术利用无线信道的随机性和不确定性，增强了通信链路的保密性，保证了合法用户间的安全通信[6-8]。在地面无线网络中，这种方法已经展现出了巨大的潜力和效果[9]。

目前，常见的 PLS 技术主要包括 PLS 编码、多天线传输和协作中继等多种手段[10-12]。差错控制码，如低密度一致校验码（LDPC, low density parity check code）和极化码已被证明能够达到信息论的安全界限，并且通过有效的编码策略可以降低信息泄露的风险[13]。例如，通过采用 LDPC 码的机制，文献[14]提出了一种多信息认证方案，能够在二进制输入窃听信道下实现同密钥的完美安全性。此外，可以利用人工噪声（AN, artificial noise）方法来保障安全通信。利用多个发送天线或者多个协作节点产生 AN，在发射者已知合法接收者的信道状态信息（CSI, channel state information）条件下，在合法信道的零空间中使用波束成形方法注入 AN，这样可以选择性地只退化窃听者的信道，而不使合法用户的信道受影响，从而保障物理层安全[15]。在地面通信环境中，信道衰落和阴影效应的多样性为 PLS 技术提供了自然的随机性基础，使得 PLS 技术得到了有效应用，展示了巨大的潜力和效果[16-19]。

然而，在星地链路中，直射路径起主导作用，且合法用户与窃听者的距离远小于星地距离，因此，可以认为窃听信道和合法用户信道是相似的。这意味着卫星到合法用户和窃听者的通信链路在信道质量上变得难以区分，进而限制了 PLS 技术在星地链路中的直接应用[20]，因此，在星地通信系统中采用 PLS 技术解决通信安全问题，仍存在着许多挑战[21]。

为了实现卫星通信的安全传输，通常需要增加额外的通信设施来辅助增强合法链路容量或降低窃听链路容量。通过利用地面基站作为卫星通信的协作中继，文献[22]提出了一种机会式用户—中继选择准则，以提高星地混合中继网络的安全性能。此外，针对星地混合网络中的无人机中继和空中窃听者，文献[23]设计了无人机中继策略，并对系统的保密容量进行了详细分析。此外，卫星和地面网络之间的相互干扰通常会降低系统性能[24]。然而，来自地面网络的绿色干扰可以通过波束成形优化来设计，在保证卫星用户和地面网络的安全速率约束的同时最小化总发射功率[25]。上述星地网络中的相关研究仅考虑了卫星或地面链路的安全性，且通常需要消耗外部资源来协助所关注的安全链路。

在星地一体化通信中，安全传输需要结合卫星通信系统的特点，研究星地融合的网络框架、波形设计等关键技术。文献[26]提出了一种基于软件定义网络（SDN, software defined network）的空地一体化网络架构。除此之外，第三代合作伙伴计划（3GPP, 3rd Generation Partnership Project）也在技术报告中对 5G 融合非地面网络中的场景部署和信道模型等方面进行了探讨[27]。然而，上述研究并未提供成熟的解决方案，星地融合网络中仍存在着许多问题待解决。星地融合网络中，卫星与地面异构网络采用频谱共享技术可以提升系统资源利用率。文献[28]考虑了一种主要卫星网络与多个次要地面网络共存的协同场景，然而，实现频谱共享的同时，会造成星地组件之间的干扰。文献[29]首次提出了基于绿色协同干扰的共生安全方案，其中，用户间干扰作为绿色干扰源来降低 Eves 的窃听能力。然而，针对星地共生安全传输模型的性能分析还较欠缺。

本文研究了星地融合网络中的下行安全传输问题，为了实现卫星与地面异构链路的安全传输，在资源受限条件下，考虑一种星地异构共生安全传输模型。星地异构共生安全传输是指卫星和地面网络的下行传输采用频谱共享的情况下，不需要额外的辅助，利用来自系统内部的互惠干扰来实现共生安全。针对窃听威胁场景下的星地安全传输需求，分析了接收端的保密速率和保密中断概率，给出了保密速率的理论下界和保密中断概率的表达式，最后通过仿真验证了理论分析的正确性，对共生安全方法的实现和优化具有一定的理论指导意义。

1　系统模型

共生安全通信模型如图 1 所示，考虑一个频谱

共享的星地融合网络[30]，在卫星S_1和基站S_2的共同覆盖范围内，存在卫星用户D_1、基站用户D_2，以及窃听者Eve。

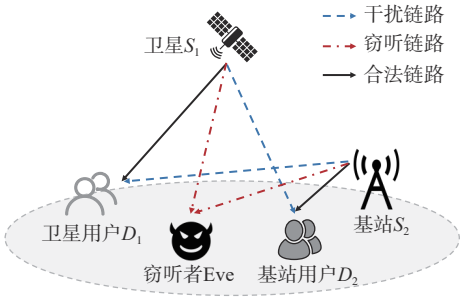

图1　共生安全通信模型

进行数据传输时，卫星S_1与基站S_2分别给对应用户发送保密信号。D_1、D_2和Eve均可以接收到来自S_1与S_2的保密信号和由于频谱共享而产生的同频干扰信号，通过合理分配资源，可以将用户通信中“废”的干扰转化为有利于对方安全传输的互惠干扰，从而实现共生安全。

D_1和D_2接收到的信号分别表示为

$$y_1 = h_{11}x_1 + h_{21}x_2 + n_1 \tag{1}$$

$$y_2 = h_{12}x_1 + h_{22}x_2 + n_2 \tag{2}$$

其中，x_1为S_1向D_1发射的保密信号，x_2为S_2向D_2发射的保密信号；n_i（$i=1,2$）为D_i（$i=1,2$）处的加性噪声；h_{11}、h_{12}、h_{21}和h_{22}为S与D之间的合法信道，假设其均为独立的瑞利信道状态变量，服从复高斯分布。

$$\begin{aligned} h_{11} &\sim \mathrm{CN}\left(0,\delta_{11}^2\right)\\ h_{12} &\sim \mathrm{CN}\left(0,\delta_{12}^2\right)\\ h_{21} &\sim \mathrm{CN}\left(0,1\right)\\ h_{22} &\sim \mathrm{CN}\left(0,1\right) \end{aligned} \tag{3}$$

其中，δ_{11}^2和δ_{12}^2分别为信道h_{11}和h_{12}的噪声功率。

基于式(1)和式(2)，用户D_1和D_2处的信干噪比（SINR, signal-to-interference-plus-noise-ratio）可以分别表示为

$$\gamma_1 = \frac{p_1|h_{11}|^2}{p_2|h_{21}|^2+\delta_1^2} \tag{4}$$

$$\gamma_2 = \frac{p_2|h_{22}|^2}{p_1|h_{12}|^2+\delta_2^2} \tag{5}$$

其中，p_1和p_2分别为S_1和S_2的发射信号功率。

同理，窃听者Eve的信号表示为

$$y_{\mathrm{e}} = h_{1\mathrm{e}}x_1 + h_{2\mathrm{e}}x_2 + n_{\mathrm{e}} \tag{6}$$

其中，$h_{1\mathrm{e}}\sim\mathrm{CN}\left(0,\delta_{1\mathrm{e}}^2\right)$，$h_{2\mathrm{e}}\sim\mathrm{CN}\left(0,1\right)$。这里考虑Eve具备攻击卫星链路或者地面链路的动机，因此，Eve试图获取卫星信号或基站信号的接收SINR分别表示为

$$\gamma_{1\mathrm{e}} = \frac{p_1|h_{1\mathrm{e}}|^2}{p_2|h_{2\mathrm{e}}|^2+\delta_{\mathrm{e}}^2} \tag{7}$$

$$\gamma_{2\mathrm{e}} = \frac{p_1|h_{2\mathrm{e}}|^2}{p_2|h_{1\mathrm{e}}|^2+\delta_{\mathrm{e}}^2} \tag{8}$$

γ_1的累积分布函数（CDF, cumulative distribution function）表示为

$$F_{\gamma_1}(\gamma) = \mathbb{P}\left(\frac{p_1|h_{11}|^2}{p_2|h_{21}|^2+\delta_1^2} \leqslant \gamma\right) \tag{9}$$

令$X=|h_{11}|^2$和$Y=|h_{21}|^2$，假设其均为独立的指数随机变量，即

$$\begin{aligned} X &\sim \mathrm{Exp}\left(\lambda_{11}\right)\\ Y &\sim \mathrm{Exp}\left(\lambda_{21}\right) \end{aligned} \tag{10}$$

其中，参数$\lambda_{11}=1/\delta_{11}$，$\lambda_{21}=1/\delta_{21}$。

因此，式(9)可以表示为

$$\begin{aligned} &F_{\gamma_1}(\gamma) = \mathbb{P}\left(\frac{p_1X}{p_2Y+\delta_1^2} \leqslant \gamma\right) =\\ &\mathbb{P}\left(X \leqslant \frac{\gamma\left(p_2Y+\delta_1^2\right)}{p_1}\right) =\\ &\int_0^{\infty}\mathbb{P}\left(X \leqslant \frac{\gamma\left(p_2y+\delta_1^2\right)}{p_1}\right)f_Y(y)\mathrm{d}y \end{aligned} \tag{11}$$

其中，$f_Y(y)$为Y的概率密度函数，表示为

$$f_Y(y) = \lambda_{21}\mathrm{e}^{-\lambda_{21}y} \tag{12}$$

因此，式(11)可以化简为

$$\begin{aligned} &F_{\gamma_1}(\gamma) = \int_0^{\infty}\left(1-\mathrm{e}^{-\lambda_{11}\frac{\gamma\left(p_2y+\delta_1^2\right)}{p_1}}\right)\lambda_{21}\mathrm{e}^{-\lambda_{21}y}\mathrm{d}y =\\ &1-\lambda_{21}\mathrm{e}^{-\lambda_{11}\frac{\gamma\delta_1^2}{p_1}}\int_0^{\infty}\mathrm{e}^{-\left(\lambda_{21}+\frac{\lambda_{11}\gamma p_2}{p_1}\right)y}\mathrm{d}y =\\ &1-\frac{\mathrm{e}^{-\lambda_{11}\frac{\gamma\delta_1^2}{p_1}}}{1+\frac{\lambda_{11}\gamma p_2}{\lambda_{21}p_1}} \end{aligned} \tag{13}$$

同理，可以得到$\gamma_{1\mathrm{e}}$的CDF为

$$F_{\gamma_{1\mathrm{e}}}(\gamma) = 1-\frac{\mathrm{e}^{-\lambda_{1\mathrm{e}}\frac{\gamma\delta_{\mathrm{e}}^2}{p_1}}}{1+\frac{\lambda_{1\mathrm{e}}\gamma p_2}{\lambda_{2\mathrm{e}}p_1}} \tag{14}$$

2　理论分析

2.1　保密速率分析

根据物理层安全理论[31]，D_1和D_2的保密速率

表示为

$$R_1 = \left[\mathrm{lb}\left(1+\gamma_1\right) - \mathrm{lb}\left(1+\gamma_{1\mathrm{e}}\right)\right]^+ \tag{15}$$

$$R_2 = \left[\mathrm{lb}\left(1+\gamma_2\right) - \mathrm{lb}\left(1+\gamma_{2\mathrm{e}}\right)\right]^+ \tag{16}$$

其中，$[x]^+ = \max(x, 0)$。D_1和D_2处的平均保密速率为

$$\bar{R}_1 = \mathbb{E}\left\{\left[\mathrm{lb}\left(1+\gamma_1\right) - \mathrm{lb}\left(1+\gamma_{1\mathrm{e}}\right)\right]^+\right\} \geqslant \mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_1\right)\right\} - \mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_{1\mathrm{e}}\right)\right\} \tag{17}$$

$$\bar{R}_2 = \mathbb{E}\left\{\left[\mathrm{lb}\left(1+\gamma_2\right) - \mathrm{lb}\left(1+\gamma_{2\mathrm{e}}\right)\right]^+\right\} \geqslant \mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_2\right)\right\} - \mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_{2\mathrm{e}}\right)\right\} \tag{18}$$

其中，$\bar{R}_1$和$\bar{R}_2$分别表示卫星用户D_1和基站用户D_2的平均可达速率。直接求解式(17)~(18)较为困难，可以使用如下近似方法。

$$\mathbb{E}\left\{\mathrm{lb}\left(1+\gamma\right)\right\} \approx \mathrm{lb}\left(1+\mathbb{E}\left\{\gamma\right\}\right) \tag{19}$$

基于式(4)，可以得到

$$\mathbb{E}\left\{\gamma_1\right\} = \frac{p_1\mathbb{E}\left\{|h_{11}|^2\right\}}{p_2\mathbb{E}\left\{|h_{21}|^2\right\}+\delta_1^2} = \frac{\dfrac{p_1}{\lambda_{11}}}{\dfrac{p_2}{\lambda_{21}}+\delta_1^2} \tag{20}$$

将式(20)代入式(19)，可得

$$\mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_1\right)\right\} \approx \mathrm{lb}\left(1+\frac{p_1\lambda_{21}}{p_2\lambda_{11}+\lambda_{11}\lambda_{21}\delta_1^2}\right) \tag{21}$$

类似地，对于$\gamma_{1\mathrm{e}}$，有

$$\mathbb{E}\left\{\mathrm{lb}\left(1+\gamma_{1\mathrm{e}}\right)\right\} \approx \mathrm{lb}\left(1+\frac{p_1\lambda_{2\mathrm{e}}}{p_2\lambda_{1\mathrm{e}}+\lambda_{1\mathrm{e}}\lambda_{2\mathrm{e}}\delta_{\mathrm{e}}^2}\right) \tag{22}$$

因此，式(17)和式(18)可以简化为

$$\bar{R}_1 \geqslant \mathrm{lb}\left(\frac{1+\dfrac{p_1\lambda_{21}}{p_2\lambda_{11}+\lambda_{11}\lambda_{21}\delta_1^2}}{1+\dfrac{p_1\lambda_{2\mathrm{e}}}{p_2\lambda_{1\mathrm{e}}+\lambda_{1\mathrm{e}}\lambda_{2\mathrm{e}}\delta_{\mathrm{e}}^2}}\right) \tag{23}$$

$$\bar{R}_2 \geqslant \mathrm{lb}\left(\frac{1+\dfrac{p_2\lambda_{12}}{p_1\lambda_{22}+\lambda_{12}\lambda_{22}\delta_2^2}}{1+\dfrac{p_2\lambda_{1\mathrm{e}}}{p_1\lambda_{2\mathrm{e}}+\lambda_{1\mathrm{e}}\lambda_{2\mathrm{e}}\delta_{\mathrm{e}}^2}}\right) \tag{24}$$

2.2　保密中断概率分析

保密中断概率（SOP, secrecy outage probability）是分析无线系统保密性能的一个关键指标[32]。较低的SOP意味着系统能够在给定条件下更好地保证通信的保密性，从而提高系统的安全性和可靠性[33-35]。通过分析和优化SOP，可以有效地评估并提升通信系统的整体保密性能。

具体而言，保密中断概率定义为瞬时保密容量低于某一阈值ϕ的概率，当瞬时保密容量低于该阈值时，通信链路的保密性无法得到有效的保障，通信被中断[36]。D_1处的保密中断概率具体表示为

$$\mathbb{P}\left\{R_1 \leqslant \phi\right\} = \mathbb{P}\left\{\gamma_1 - \varphi\gamma_{1\mathrm{e}} \leqslant \varphi - 1\right\} \triangleq \mathbb{P}_{\mathrm{out}} \tag{25}$$

其中，$\mathrm{lb}(\varphi) = \phi$。

为了计算保密中断概率，需要计算不等式$\gamma_1 - \varphi\gamma_{1\mathrm{e}} \leqslant \varphi - 1$成立的概率。这需要找到$\gamma_1$和$\gamma_{1\mathrm{e}}$的联合概率密度函数（PDF, probability density function），然后在不等式定义的区域内对PDF进行积分。假设γ_1和$\gamma_{1\mathrm{e}}$是独立的，则式(25)可以表示为

$$\mathbb{P}_{\mathrm{out}} = F_{\gamma_1}\left(\varphi\gamma_{1\mathrm{e}} + \varphi - 1\right) \tag{26}$$

因此，有

$$\mathbb{P}_{\mathrm{out}} = \int_0^\infty \left(1 - \frac{\mathrm{e}^{-\lambda_{11}\frac{\left(\varphi\gamma_{1\mathrm{e}}+\varphi-1\right)\delta_1^2}{p_1}}}{1+\dfrac{\lambda_{11}\left(\varphi\gamma_{1\mathrm{e}}+\varphi-1\right)p_2}{\lambda_{21}p_1}}\right) f_{\gamma_{1\mathrm{e}}}\left(\gamma_{1\mathrm{e}}\right)\mathrm{d}\gamma_{1\mathrm{e}} = \int_0^\infty \left(1 - \frac{\mathrm{e}^{-\lambda_{11}\frac{\left(\varphi\gamma_{1\mathrm{e}}+\varphi-1\right)\delta_1^2}{p_1}}}{1+\dfrac{\lambda_{11}\left(\varphi\gamma_{1\mathrm{e}}+\varphi-1\right)p_2}{\lambda_{21}p_1}}\right)\lambda_{1\mathrm{e}}\mathrm{e}^{-\lambda_{1\mathrm{e}}\gamma_{1\mathrm{e}}}\mathrm{d}\gamma_{1\mathrm{e}} \tag{27}$$

令$u = \gamma_{1\mathrm{e}}$，可得

$$\mathbb{P}_{\mathrm{out}} = \int_0^\infty \left(1 - \frac{\mathrm{e}^{-\lambda_{11}\frac{(\varphi u+\varphi-1)\delta_1^2}{p_1}}}{1+\dfrac{\lambda_{11}(\varphi u+\varphi-1)p_2}{\lambda_{21}p_1}}\right)\lambda_{1\mathrm{e}}\mathrm{e}^{-\lambda_{1\mathrm{e}}u}\mathrm{d}u = 1 - \int_0^\infty \frac{\lambda_{1\mathrm{e}}\mathrm{e}^{-\left(\lambda_{1\mathrm{e}}+\lambda_{11}\frac{\varphi\delta_1^2}{p_1}\right)u}\mathrm{e}^{-\lambda_{11}\frac{(\varphi-1)\delta_1^2}{p_1}}}{1+\dfrac{\lambda_{11}(\varphi u+\varphi-1)p_2}{\lambda_{21}p_1}}\mathrm{d}u \tag{28}$$

令$c = \lambda_{1\mathrm{e}} + \lambda_{11}\varphi\delta_1^2/p_1$，则

$$\mathbb{P}_{\mathrm{out}}^1 = 1 - \mathrm{e}^{-\lambda_{11}\frac{(\varphi-1)\delta_1^2}{p_1}}\int_0^\infty \frac{\lambda_{1\mathrm{e}}\mathrm{e}^{-cu}}{1+\dfrac{\lambda_{11}(\varphi u+\varphi-1)p_2}{\lambda_{21}p_1}}\mathrm{d}u = 1 - \mathrm{e}^{-\lambda_{11}\frac{(\varphi-1)\delta_1^2}{p_1}}\frac{\lambda_{21}p_1}{\lambda_{11}\varphi p_2}\mathrm{e}^{\frac{c\lambda_{12}p_1}{\lambda_{11}\varphi p_2}}\mathrm{Ei}\left(-\frac{c\lambda_{21}p_1}{\lambda_{11}\varphi p_2}\right) \tag{29}$$

其中，$\mathrm{Ei}(x)$为指数积分函数

$$\mathrm{Ei}(x) = -\int_{-x}^\infty \frac{\mathrm{e}^{-t}}{t}\mathrm{d}t \tag{30}$$

同理，可以得到D_2的保密中断概率为

$$\mathbb{P}_{\mathrm{out}}^2 = 1 - \mathrm{e}^{-\lambda_{22}\frac{(\varphi-1)\delta_2^2}{p_2}}\frac{\lambda_{12}p_2}{\lambda_{22}\varphi p_1}\mathrm{e}^{\frac{c\lambda_{12}p_2}{\lambda_{22}\varphi p_1}}\mathrm{Ei}\left(-\frac{c\lambda_{12}p_2}{\lambda_{22}\varphi p_1}\right) \tag{31}$$

其中，$c = \lambda_{2\mathrm{e}} + \lambda_{22}\varphi\delta_2^2/p_2$。

3　仿真结果

为了验证异构融合通信中共生安全系统的保密性能，通过对不同阈值和功率分配下的保密中断概率进行蒙特卡洛仿真来比较保密性能。

首先对保密速率下界进行模拟仿真，多用户协作下保密速率与功率的关系如图2所示，为保密速率R_1与R_2随着发射功率p_1的变化曲线。假设发射功率p_1为0 dB到18 dB，系统平均信道增益参数$\lambda_{12}=\lambda_{21}=2$，$\lambda_{1e}=\lambda_{2e}=4$，$\lambda_{11}=\lambda_{22}=5$，噪声功率$\delta_1^2=\delta_2^2=1$。

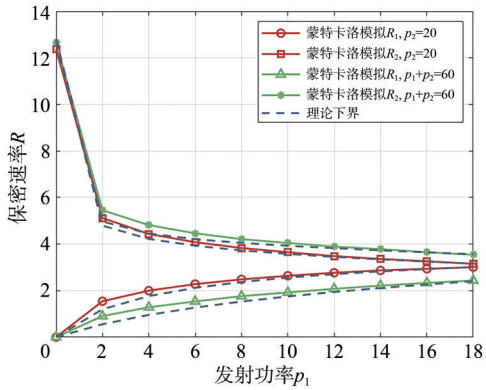

图2　多用户协作下保密速率与功率的关系

从图2可以得到以下结论：1) 保密速率的理论下界与蒙特卡洛模拟结果接近，验证了保密速率理论下界分析结果的正确性；2) 合法用户的保密速率在不同发射功率下均为正值，证明了共生安全系统的保密性能。R_1随着p_1的增加而增加，R_2随着p_1的增加而减少，这是因为在频谱共享环境中，卫星用户信号增强，抑制了基站用户的信号质量，从而降低了保密速率R_2。

保密中断概率与总功率的关系如图3所示，为卫星用户D_1和基站用户D_2的保密中断概率随总发射功率的变化曲线。从图3可以看出，随着总发射功率的增加，系统的保密中断概率减小，保密性能提升，这是因为下行链路增加的协作干扰使得窃听作用随着总功率的增加而降低。保密中断概率与保密阈值的关系如图4所示，结合图4保密中断概率与保密阈值的变化曲线，可以得知，随着保密阈值的增加，保密中断概率变大。这是因为随着保密阈值的增加，系统对信号强度的要求提高，导致信号必须显著超过噪声和干扰才能保证保密性，窃听者在强噪声环境下仍可能接收到足够的信息，从而导致保密中断。

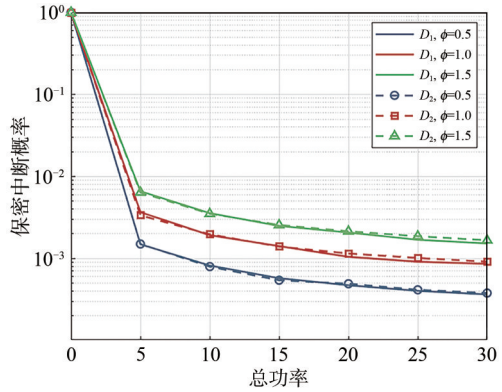

图3　保密中断概率与总功率的关系

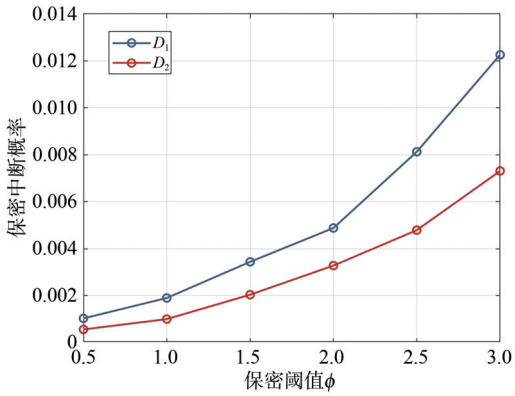

图4　保密中断概率与保密阈值的关系

4　结束语

本文研究了星地融合通信中共生安全的保密性能，考虑了一种共生安全通信框架，利用来自系统内部的异构互惠干扰来实现共生安全。通过理论推导分析了星地异构链路的保密速率下界和保密中断概率。仿真结果验证了理论分析的正确性，研究结果表明，随着总发射功率的增加，系统的保密中断概率显著降低，证明了共生安全策略在提高星地通信安全性方面的有效性。此外，可以采用信号处理的方法，如波束成形和安全编码等方法，通过优化互惠干扰，在高动态环境中实现可靠和高效的通信安全传输。本文为星地融合网络中的物理层安全提供了有效的解决方案，对未来的星地通信安全设计具有一定意义。

参考文献：

[1] 徐玺贺, 台祥雪, 韩帅, 等. 卫星通信网络基于保密中断概率最小化的功率分配方案[J]. 移动通信, 2018, 42(7): 66-70, 76.
XU X H, TAI X X, HAN S, et al. Power allocation based on the

minimization of secrecy outage probability for satellite communication networks[J]. Mobile Communications, 2018, 42(7): 66-70, 76.

[2] LIN X D, LU R X, SHEN X M, et al. Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems[J]. IEEE Journal on Selected Areas in Communications, 2009, 27(4): 365-378.

[3] ZHU F C, YAO M L. Improving physical-layer security for CRNs using SINR-based cooperative beamforming[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1835-1841.

[4] TASHMAN D H, HAMOUDA W. An overview and future directions on physical-layer security for cognitive radio networks[J]. IEEE Network, 2021, 35(3): 205-211.

[5] XU W J, LI S Y, LEE C H, et al. Optimal secure multicast with simultaneous wireless information and power transfer in presence of multiparty eavesdropper collusion[J]. IEEE Transactions on Vehicular Technology, 2016, 65(11): 9123-9137.

[6] LIU Y L, CHEN H H, WANG L M. Secrecy capacity analysis of artificial noisy MIMO channels—an approach based on ordered eigenvalues of wishart matrices[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(3): 617-630.

[7] WANG W, TEH K C, LUO S, et al. Physical layer security in heterogeneous networks with pilot attack: a stochastic geometry approach[J]. IEEE Transactions on Communications, 2018, 66(12): 6437-6449.

[8] YANG X, SHU L, LIU Y, et al. Physical security and safety of IoT equipment: a survey of recent advances and opportunities[J]. IEEE Transactions on Industrial Informatics, 2022, 18(7): 4319-4330.

[9] WU Y P, KHISTI A, XIAO C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 679-695.

[10] ALI MEMON M, RAMAYAH T, CHEAH J H, et al. PLS-SEM statistical programs: a review[J]. Journal of Applied Structural Equation Modeling, 2021, 5(1): 1-14.

[11] PURWANTO A. Partial least squares structural equation modeling (PLS-SEM) analysis for social and management research: a literature review[J]. Journal of Industrial Engineering & Management Research, 2021, 2(4): 114-123.

[12] BECKER J M, CHEAH J H, GHOLAMZADE R, et al. PLS-SEM's most wanted guidance[J]. International Journal of Contemporary Hospitality Management, 2023, 35(1): 321-346.

[13] BLOCH M, HAYASHI M, THANGARAJ A. Error-control coding for physical-layer secrecy[J]. Proceedings of the IEEE, 2015, 103(10): 1725-1746.

[14] CHEN D J, ZHANG N, LU R X, et al. An LDPC code based physical layer message authentication scheme with prefect security[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 748-761.

[15] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[16] BLOCH M, GÜNLÜ O, YENER A, et al. An overview of information-theoretic security and privacy: metrics, limits and applications[J]. IEEE Journal on Selected Areas in Information Theory, 2021, 2(1): 5-22.

[17] ARFAOUI M A, SOLTANI M D, TAVAKKOLNIA I, et al. Physical layer security for visible light communication systems: a survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1887-1908.

[18] ZHANG J Y, DU H Y, SUN Q, et al. Physical layer security enhancement with reconfigurable intelligent surface-aided networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3480-3495.

[19] WANG W, TEH K C, LI K H. Artificial noise aided physical layer security in multi-antenna small-cell networks[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1470-1482.

[20] YIN Z S, CHENG N, LUAN T H, et al. DT-assisted multi-point symbiotic security in space-air-ground integrated networks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5721-5734.

[21] HAN S, LI J X, MENG W X, et al. Challenges of physical layer security in a satellite-terrestrial network[J]. IEEE Network, 2022, 36(3): 98-104.

[22] BANKEY V, UPADHYAY P K. Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2488-2501.

[23] SHARMA P K, KIM D I. Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks[J]. IEEE Transactions on Wireless Communications, 2020, 19(4): 2770-2784.

[24] LIN Z, LIN M, DE COLA T, et al. Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks[J]. IEEE Internet of Things Journal, 2021, 8(14): 11123-11134.

[25] LIN M, LIN Z, ZHU W P, et al. Joint beamforming for secure communication in cognitive satellite terrestrial networks[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(5): 1017-1029.

[26] ZHU X M, JIANG C X. Integrated satellite-terrestrial networks toward 6G: architectures, applications, and challenges[J]. IEEE Internet of Things Journal, 2022, 9(1): 437-461.

[27] 3GPP. 3rd Generation Partnership Project; Technical specification group services and system aspects; Release18 description; summary of Rel-18 work items (Release 18: TR 21.918)[S]. 2024.

[28] CHEN Z Y, GUO D X, DING G R, et al. Optimized power control scheme for global throughput of cognitive satellite-terrestrial networks based on non-cooperative game[J]. IEEE Access, 2019, 7: 81652-81663.

[29] YIN Z S, CHENG N, LUAN T H, et al. Green interference based symbiotic security in integrated satellite-terrestrial communications[J]. IEEE Transactions on Wireless Communications, 2022, 21(11): 9962-9973.

[30] LI C X, GUAN L, WU H Q, et al. Dynamic spectrum control-assisted secure and efficient transmission scheme in heterogeneous cellular networks[J]. Engineering, 2022, 17: 220-231.
[31] BESSER K L, JORSWIECK E A. Bounds on the secrecy outage probability for dependent fading channels[J]. IEEE Transactions on Communications, 2021, 69(1): 443-456.
[32] ZHANG Y Q, YE J, PAN G F, et al. Secrecy outage analysis for satellite-terrestrial downlink transmissions[J]. IEEE Wireless Communications Letters, 2020, 9(10): 1643-1647.
[33] LIU Y L, SU Z, ZHANG C, et al. Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted MIMOME system[J]. IEEE Transactions on Wireless Communications, 2023, 22(2): 1374-1387.
[34] BAO T N, ZHU J, YANG H C, et al. Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation[J]. IEEE Wireless Communications Letters, 2020, 9(9): 1351-1355.
[35] YIN Z S, JIA M, WANG W, et al. Secrecy rate analysis of satellite communications with frequency domain NOMA[J]. IEEE Transactions on Vehicular Technology, 2019, 68(12): 11847-11858.
[36] BLOCH M, BARROS J. Physical-layer security: from information theory to security engineering[M]. New York: Cambridge University Press, 2011.

[作者简介]

赵璇（2002– ），女，西安电子科技大学网络与信息安全学院硕士生，主要研究方向为无线通信系统、网络空间安全、空天地一体化网络安全等。

尹志胜（1990– ），男，西安电子科技大学通信工程学院副教授、硕士生导师，主要研究方向为空天地一体化网络、无线通信系统、面向6G的星地一体高效接入与传输技术、星地物理层安全通信方法、智能传输技术等。

承楠（1987– ），男，西安电子科技大学通信工程学院教授、博士生导师，主要研究方向为智能车联网及先进交通系统、空天地一体化网络、人工智能与大数据技术在网络中的应用。

刘永红（2002– ），男，西安电子科技大学网络与信息安全学院硕士生，主要研究方向为无线通信与系统、网络空间安全、空天地一体化网络安全等。

王兆薇（2000– ），女，西安电子科技大学通信工程学院博士生，主要研究方向为空天地一体化网络、物理层安全、智能传输等。