卫星地面融合网络的窃听威胁与物理层安全解决方案

Interception Threats and Physical Layer Security Solution of Integrated Satellite-Terrestrial Networks

韩帅/HAN Shuai[1]，李季蹊/LI Jixi[1]，李静涛/LI Jingtao[2]

（1. 哈尔滨工业大学，中国 哈尔滨 150000；
2. 中国空间技术研究院，中国 北京 100081）
(1. Harbin Institute of Technology, Harbin 150000, China;
2. China Academy of Space Technology, Beijing 100081, China)

摘要：分析了卫星地面融合网络（ISTN）中的现有安全架构与潜在的安全威胁。针对低轨卫星星座场景，以频发的窃听威胁作为研究重点；针对ISTN中的窃听威胁，提出了基于物理层安全（PLS）的解决方案；针对ISTN应用物理层安全解决方案所面临的相关信道、同频干扰、邻频干扰以及多用户多窃听者场景等挑战，提出了相应的解决方案。这对中国卫星互联网设施建设的落地具有重大的现实意义。

关键词：卫星地面融合网络；窃听威胁；物理层安全

Abstract: The existing security architecture and potential threats in the integrated satellite–terrestrial networks (ISTNs) are analyzed. Considering the Low Earth Orbit (LEO) satellite constellation scenario, the frequent interception threats are selected as the research focus. In view of the interception threat, solutions based on physical layer security (PLS) are proposed. The challenges of applying PLS to an ISTN, including correlated channels, co–channel interference, adjacent channel interference, and multi–user multi–eavesdropper scenarios are proposed, and the corresponding solutions to these challenges are then analyzed. This is of great practical significance to the construction of China's satellite Internet facilities.

Keywords: integrated satellite–terrestrial networks; interception threats; physical layer security

DOI：10.12142/ZTETJ.202105009
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20210930.1238.002.html

网络出版日期：2021–09–30
收稿日期：2021–08–16

由于卫星网络业务具有广播特性，数据会传递给一定范围内的多个接收者，包括合法用户以及非法用户，因此每个合法用户都会受到不同程度的安全和隐私威胁。工作中的卫星很难进行安全漏洞修补，因此我们需要预先对卫星地面融合网络（ISTN）可能面对的安全威胁进行分类评估，并提出相应的安全方案以对抗潜在的安全威胁。

低轨（LEO）卫星星座在保证与地球同步轨道卫星同样的覆盖范围的前提下，大幅降低了通信的往返时延，是ISTN的重要组成部分。虽然单个LEO卫星仍然只能在短时间内可见，但这并不意味着其安全性得到了提高。因为对卫星星座所形成的在轨网络而言，星座中的每颗卫星都充当了其相邻卫星的路由中继，从而增加了整个星座的安全风险。

1 ISTN的安全风险与现有安全架构

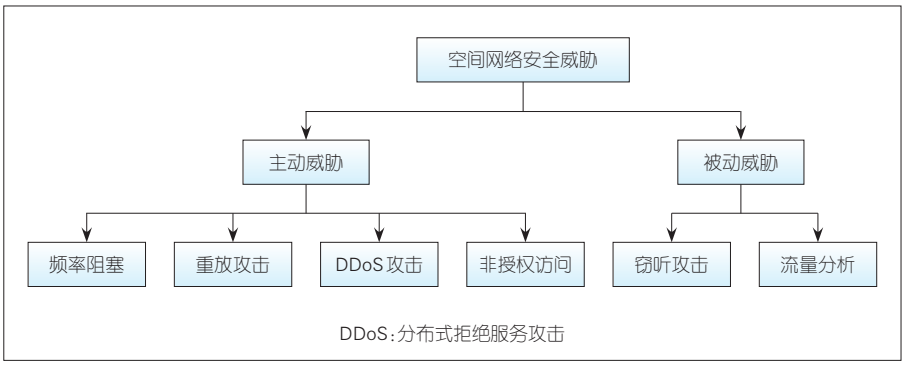
目前，关于ISTN安全架构的主流观点是基于2012年国际空间数据系统咨询委员会（CCSDS）提出的空间网络安全架构的。CCSDS将安全威胁分为两部分：主动威胁与被动威胁。主动威胁包括频率阻塞攻击、重放攻击、分布式拒绝服务攻击（DDoS）

基金项目：国家自然科学基金（61831002、61771169）

攻击以及非授权访问攻击，被动威胁包括窃听以及流量分析。这两种威胁均可以出现在卫星通信的空间段、地面段以及空间传输链路等处，其分类如图1所示。

在频率阻塞攻击中，通过在相同频率上发射大功率噪声，攻击者造成了严重的链路损耗，并阻断星地通信接入。重放攻击是指攻击者重复向卫星传输之前拦截并记录的指令。若重放指令未被拒绝，则卫星有可能重复执行操作，这会导致卫星偏离轨道或天线指向错误。不同于上述偏向物理层的安全威胁，DDoS攻击主要来自于网络层的瞬时海量访问攻击，它通过阻塞合法用户的接入达到拒绝服务的目的。非授权访问攻击是指未授权用户假冒合法用户对网络中的节点进行访问。在2003年，中国“鑫诺卫星”的转发器就曾遭到以大功率信号伪装成卫星地球站的境外势力的劫持，播出了非法信号，造成了极为恶劣的影响。在被动威胁中，攻击者可以在不被察觉的情况下，窃听卫星广播信号。此外，攻击者还可以通过分析卫星通信流量，侵害用户的隐私。

CCSDS的安全架构主要考虑3点：物理安全、信息安全（数据的机密性、完整性）以及传输安全（隐藏通信链路，防止被阻塞）。卫星通信管理部门可以根据通信任务的不同，在不同层协议中进行加密，以保证信息的保密性、完整性。在安全级别更高的通信任务中，可以应用物理层加密，以对抗流量分析等被动威胁。在LEO卫星星座与5G融合的场景下，海量接入用户与星间链路的存在导致上述安全威胁中的窃听攻击变得更为频繁，因此，我们将主要讨论针对窃听攻击的解决方案。



▲图1 空间网络威胁分类

2 窃听威胁及其解决方案

2.1 物理层安全技术概述

卫星通信的广播特性决定了其信息极易被窃听，A.D.Wyner在文献[1]中建立了如图2所示的窃听信道模型。其中，X,Y,Z分别为信源发射的信号和用户与窃听者接收的信号，h_m,h_e分别为主信道与窃听信道的信道系数，γ_m,γ_e分别表示用户与窃听者处的信干噪比。在文献[1]中，A.D.Wyner证明了当窃听链路信干噪比比主信道的信干噪比差时，保密容量C_s满足式(1)：

$$C_s=\left[C_m-C_e\right]^+=\left[\log_2\left(1+\gamma_m\right)-\log_2\left(1+\gamma_e\right)\right]^+。\quad(1)$$

当保密容量非负时，合法用户正常接收信号，而窃听者获得保密信息的概率为0。

显而易见，在A.D.Wyner所提的窃听信道模型中，当保密容量为0（即$\gamma_m\leqslant\gamma_e$）时，系统不能保证完美的保密性。此时进行信息传输则很有可能被窃听者成功窃听，从而导致保密信息泄露。而物理层安全技术正是通过已知的信道信息h_m、h_e，绕过密钥加密，通过预编码等物理层技术，最大化保密容量以保证安全传输。

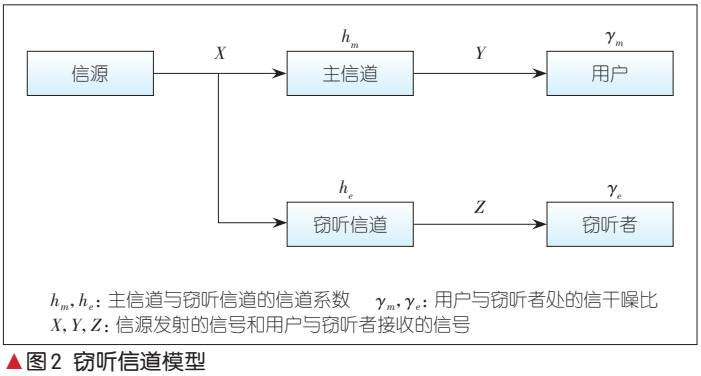
物理层安全是一种基于无线信道特性对信息传输进行加密的技术。作为一种全新的安全架构，物理层安全技术有许多优点：

（1）物理层安全利用无线信道的天然随机性和复杂性，可以实现“一次一密”保证安全通信。

（2）物理层安全技术主要用于物理层，无须考虑上层协议，可以作为传统加密方式的补充，以增强传统加密协议的综合性能。

（3）密钥加密有被量子计算破解的风险，而物理层安全技术则通过无线信道的随机性规避了这一问题。

可以预见，物理层安全技术将会作为CCSDS安全协议的补充，与地面核心网的安全架构进一步融合，形成



▲图2 窃听信道模型

全新的ISTN安全架构。目前，关于物理层安全的研究主要集中于资源分配[2-4]、波束成形与人工噪声[5-6]、用户节点选择与协作[7-8]三大类技术。这3类技术的本质都是通过预编码、协作干扰等物理层手段，降低窃听者处的信干噪比或提高合法用户处的信干噪比，以保证非负的保密速率。目前相关的理论研究已经较为成熟。

目前，也有部分研究[9-10]将物理层安全技术拓展至ISTN场景中，研究卫星与地面节点的预编码与协作调度方案。将地面的物理层安全技术从地面移植到卫星上并不简单，因为卫星信道更为复杂，衰减更为严重，且通信距离较远。利用信道的特性来保证安全传输，可能会面临诸多挑战。

（1）相关信道

在ISTN场景中，合法用户的信道h_m与窃听信道h_e的相关性将远高于传统的地面场景，因此传统的物理层安全方法在卫星场景下有失效之虞。

（2）同频干扰与邻频干扰

中国地面5G蜂窝通信主要工作于5G频谱n78频带中的3.4~3.6 GHz频段，但3.4~4.2 GHz频段已经被国际电信联盟分配给了卫星通信业务，共享的频谱将在3.4~3.6 GHz频段与3.6~4.2 GHz频段内引入严重的同频干扰和邻频干扰。这种干扰对依赖于无线信道特性的物理层安全技术也将是一个严重的打击。

（3）多用户多窃听者场景

在ISTN场景中，卫星往往需要为数量远多于地面场景的用户提供服务，ISTN要应对的窃听者的数量也会大幅度增加。为对抗多窃听者空间分集导致的窃听信干噪比增益，我们需要在ISTN中应用更加灵活的物理层安全技术。

2.2 物理层安全在ISTN中遇到的挑战

2.2.1 相关信道

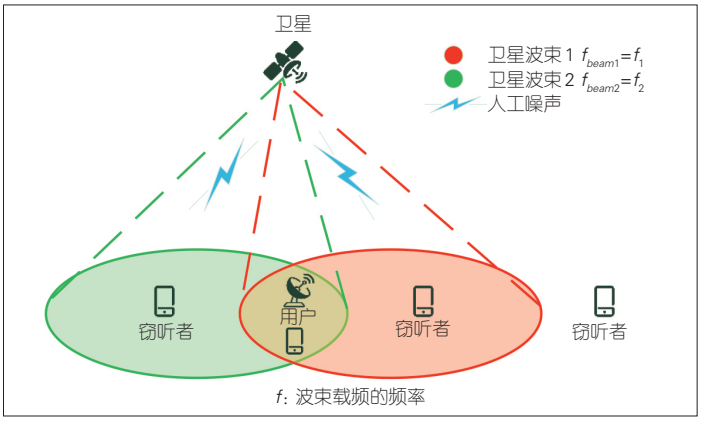
卫星和终端之间的距离较大，而窃听者与用户之间的距离可以忽略不计。因此，用户和窃听者之间信道的相关性较高。当窃听者靠近合法接收者时，即便已经采用了人工噪声和波束成形等传统物理层安全方案，卫星和用户通信的保密能力还会迅速降低。这使得我们不得不采取其他方法来扩大窃听信道与主信道之间的差异。

文献[11]引入了双频双波束的传输方案，以扩大主信道与保密信道的差异。如图3所示，用户由不同频率的两个波束提供服务，每个波束的功率都是单波束场景的一半。此外，我们还证明了这种双频双波束的传输方案存在最优的波束成形与人工噪声矢量，可以保证窃听者与用户间距离较小时的高保密速率。

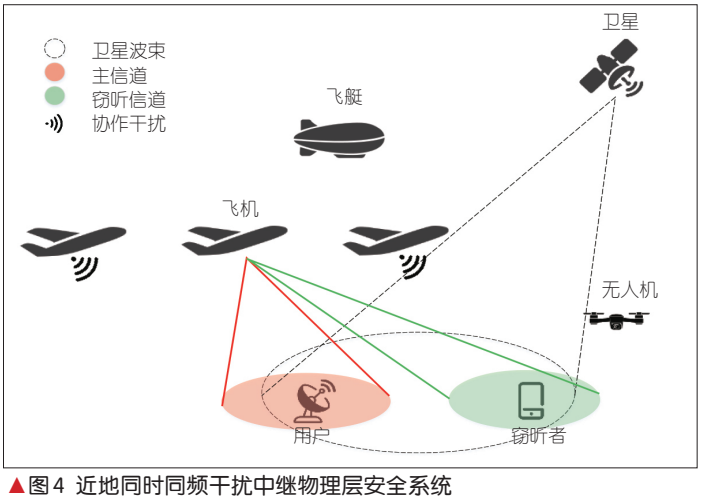
文献[12]假设了一个带有近地中继的ISTN，如图4所示。如上文所述，即便是LEO卫星，其波束的覆盖范围也在200 km左右，窃听者与用户极有可能被同一波束覆盖，两者之间的信道相关性较高。近地中继（如飞机、飞艇等航空器）的波束覆盖范围较小，窃听者与用户信道会产生很大的差异，从而给物理层安全技术留下了发挥的空间。在此基础上，我们进一步研究了近地中继的中继选择、同时同频干扰中继与卫星之间的功率分配，以优化系统的保密性能。

2.2.2 同频干扰与邻频干扰

由于卫星通信的频谱资源利用不足，且地面频谱资源日益紧张，因此，将频谱共享方法纳入ISTN的研究范畴具有广阔的前景。近年来，认知卫星地面网络的混合架构被认为是提高频谱效率的主要方案之一。该技术在地面网络和卫星网络之间共享C波段（4~8 GHz）。频谱共享缓解了频谱稀缺问题，但又会面临着另外



▲图3 双频双波束物理层安全卫星地面融合网络



▲图4 近地同时同频干扰中继物理层安全系统

一个困扰，即卫星和地面系统之间的同频干扰与邻频干扰。这种卫星业务与5G系统间的频率冲突会导致星地链路信干噪比、保密容量等指标降低，从而影响通信质量。除此之外，在第3代合作伙伴计划（3GPP）R17规划中的卫星物联网也同样面临着由于海量接入而引发的干扰问题。在现行的干扰协调指南中，我们通常使用频率隔离、地理隔离，以及加装滤波器、屏蔽网等方案减轻干扰。本文中，基于物理层安全的解决方案，我们可以通过波束成形与预编码等技术充分利用干扰，恶化窃听者的信道条件，降低窃听者处的信干噪比。

在认知卫星地面网络架构中，我们一般认为卫星网络是主要网络，地面网络是辅助网络。辅助网络对主信道的干扰会明显降低系统性能，如图5所示。如果将辅助网络引入的干扰视为对窃听者的干扰，那么通过波束成形来减轻对合法用户的同频干扰，就可以提升系统的保密性能。

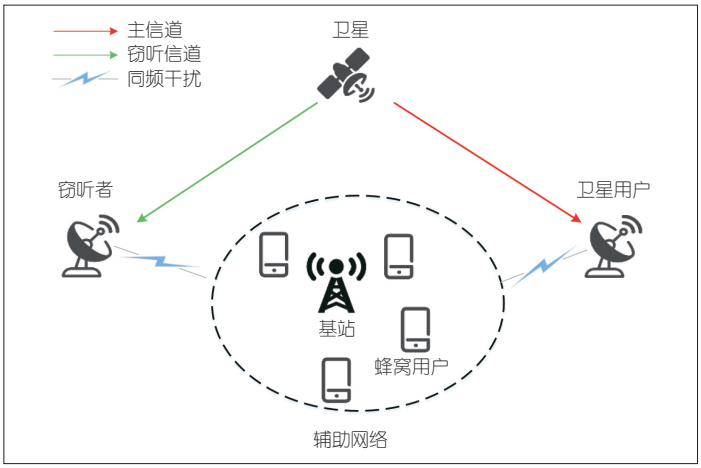
文献[13]研究了认知卫星地面网络架构中地面基站的波束成形方法，在满足主要网络（卫星网络）的保密速率约束以及辅助网络（地面网络）的通信速率约束条件的同时，最小化地面基站上的发射功率。在其基础上，文献[14]在多地面基站的场景下进一步考虑了整个系统的能效。在迫零（ZF）波束成形之外，该文献还考虑了添加人工噪声以增强系统的物理层安全的方法。

在3GPP的规划中，毫米波波段也将成为地面和卫星网络的共享波段。在毫米波信道下，部分研究着眼于卫星与地面网络，并关注波束成形方案。文献[15-16]研究了一种协作安全传输波束成形方案，通过卫星处的自适应波束成形、人工噪声以及地面基站处的波束成形的协作实现安全传输。

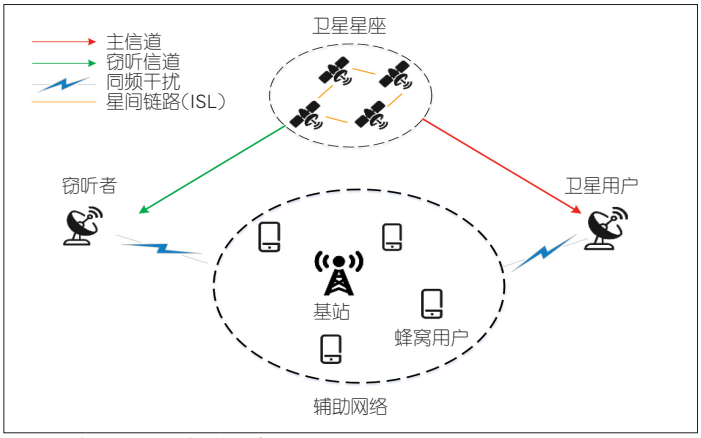
如果考虑多卫星的场景，那么就可以从另一角度——多卫星调度，来考虑频谱共享下的ISTN的物理层安全。文献[17]讨论了多卫星轮流访问共享频谱的轮询卫星调度（RSS）与多卫星共同访问共享频谱的多卫星调度（MSS），如图6所示。文献[17]分析了MSS方案的安全可靠性折衷（SRT），其中安全性和可靠性由拦截概率和中断概率来表征。面对系统保密性能过剩的问题，我们可以通过增减卫星数量来达到安全可靠性的折衷。

2.2.3 多用户多窃听者场景

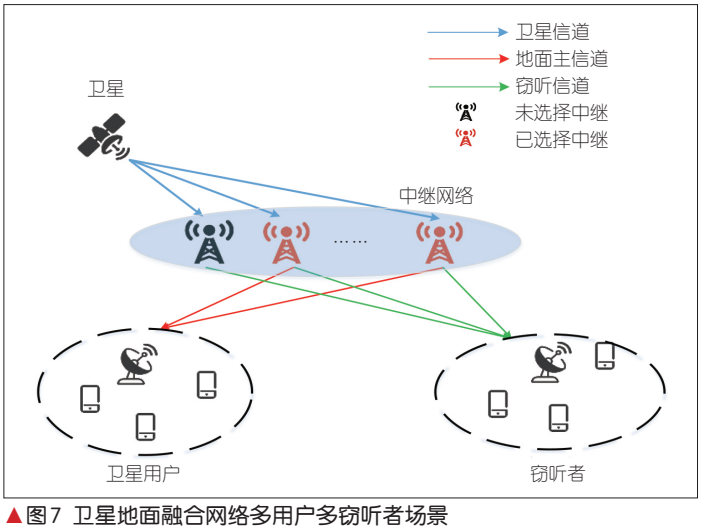
随着卫星的能力变得越来越强大，可服务的用户密度也在不断增大，这使得一个卫星波束中通常存在多个用户或窃听者。目前，多用户场景已经成为卫星地面通信网络常用的场景之一，如图7所示。与上述情况考虑的单用户单窃听者场景不同，多用户场景由于通信链路的增加，所面临的窃听风险也会不断增大。与此同时，多用户场景的空间分集也为



▲图5 认知卫星地面网络物理层安全模型



▲图6 多卫星调度频谱共享物理层安全模型



▲图7 卫星地面融合网络多用户多窃听者场景

从物理层安全角度提高系统的安全性提供了新的思路。

在多用户ISTN中，文献[18]研究了多用户协作与调度对物理层安全的增强。在混合卫星地面中继网络（HSTRN）中，其用户与中继均可以通过最大化端到端保密容量等类似的方法进行选择，以增强物理层安全性，从而逐渐成为最常用的架构之一。文献[19]推导了HSTRN中使用不同中继选择方法在放大转发与解码转发协议下的保密中断概率（SOP）。文献[20]分析了在放大转发（AF）和解码转发（DF）中继协议下具有多天线卫星的下行链路多用户多中继HSTRN的保密性能，提出了最佳用户中继对选择准则，以期使HSTRN系统的SOP最小化。

3 结束语

卫星地面融合网络是中国通信网络基础设施体系建设的重大需求。研究ISTN场景下面临的窃听威胁与解决方案，将驱动中国天地一体化信息系统的广泛应用。本文中，我们分析了ISTN在LEO卫星场景下的安全威胁与相应的解决方案，对中国卫星互联网设施建设的落地具有重大的现实意义。

致谢

感谢中国空间技术研究院和中国科学院微小卫星创新研究院对本研究的帮助。

参考文献

[1] WYNER A D. The wire-tap channel [J]. Bell system technical journal, 1975, 54(8): 1355-1387. DOI: 10.1002/j. 1538-7305.1975.tb02040.x
[2] LEE J H. Optimal power allocation for physical layer security in multi-hop DF relay networks [J]. IEEE transactions on wireless communications, 2016, 15(1): 28-38. DOI: 10.1109/TWC.2015.2466091
[3] WANG X W, TAO M X, MO J H, et al. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks [J]. IEEE transactions on information forensics and security, 2011, 6(3): 693-702. DOI:10.1109/TIFS.2011.2159206
[4] WANG J H, HUANG Y M, JIN S, et al. Resource management for device-to-device communication: a physical layer security perspective [J]. IEEE journal on selected areas in communications, 2018, 36(4): 946-960. DOI: 10.1109/JSAC.2018.2825484
[5] ZHANG W, CHEN J, KUO Y H, et al. Artificial-noise-aided optimal beamforming in layered physical layer security [J]. IEEE communications letters, 2019, 23(1): 72-75. DOI:10.1109/LCOMM.2018.2881182
[6] 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. DOI:10.1109/TIFS.2017.2663336
[7] YAN P S, ZOU Y L, ZHU J. Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems [J]. IEEE transactions on vehicular technology, 2018, 67(3): 2084-2096. DOI: 10.1109/TVT.2017.2725989
[8] ZOU Y L, WANG X B, SHEN W M. Physical-layer security with multiuser scheduling in cognitive radio networks [J]. IEEE transactions on communications, 2013, 61(12): 5103-5113. DOI:10.1109/TCOMM.2013.111213.130235
[9] 肖叶秋, 祝幸辉, 赵双睿, 等. 卫星通信系统的物理层安全性能分析 [J]. 西安电子科技大学学报, 2021, 48(3): 163-169. DOI: 10.19665/j.issn1001-2400.2021.03.021
[10] 顾晨伟, 林志, 林敏, 等. 卫星通信下行链路鲁棒安全波束成形设计 [J]. 系统工程与电子技术, 2021, 43: 1361-1370
[11] WANG P R, NI Z Y, JIANG C X, et al. Dual-beam dual-frequency secure transmission for downlink satellite communication systems [C]// 2019 IEEE Globecom Workshops (GC Wkshps). Waikoloa, HI, USA: IEEE, 2019: 1-6. DOI:10.1109/GCWkshps45667.2019.9024580
[12] LI J T, HAN S, TAI X X, et al. Physical layer security enhancement for satellite communication among similar channels: relay selection and power allocation [J]. IEEE systems journal, 2020, 14(1): 433-444. DOI: 10.1109/JSYST.2019.2921306
[13] LU W X, AN K, YAN X J, et al. Power-efficient secure beamforming in cognitive satellite-terrestrial networks [C]//2019 27th European Signal Processing Conference (EUSIPCO). A Coruna, Spain: IEEE, 2019. DOI: 10.23919/eusipco.2019.8903182
[14] LU W X, LIANG T, AN K, et al. Secure beamforming and artificial noise algorithms in cognitive satellite-terrestrial networks with multiple eavesdroppers [J]. IEEE access, 2018, 6: 65760-65771. DOI: 10.1109/ACCESS.2018.2878415
[15] DU J, JIANG C X, ZHANG H J, et al. Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming [J]. IEEE journal on selected areas in communications, 2018, 36(7): 1367-1382. DOI:10.1109/JSAC.2018.2824623
[16] 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. DOI:10.1109/JSAC.2018.2832819
[17] DING X J, ZHANG G X, QU D X, et al. Security-reliability tradeoff analysis of spectrum-sharing aided satellite-terrestrial networks [C]// 2019 IEEE Globecom Workshops (GC Wkshps). Waikoloa, HI, USA: IEEE, 2019: 1-6. DOI:10.1109/GCWkshps45667.2019.9024465
[18] GUO K F, LIN M, ZHANG B N, et al. Secrecy performance of satellite wiretap channels with multi-user opportunistic scheduling [J]. IEEE wireless communications letters, 2018, 7(6): 1054-1057. DOI: 10.1109/LWC.2018.2859385
[19] BANKEY V, UPADHYAY P K. Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes [C]//2017 IEEE 85th Vehicular Technology Conference (VTC Spring). Sydney, NSW, Australia: IEEE, 2017: 1-5. DOI: 10.1109/VTCSpring.2017.8108272
[20] 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. DOI:10.1109/TVT.2019.2893366

作 者 简 介

韩帅，哈尔滨工业大学教授；主要研究方向为无线信号处理、MIMO、非正交多址接入和卫星定位导航及对抗等；近年来先后主持了国家自然科学基金青年项目、国家自然科学基金面上项目、中央高校基本科研业务费重大专项资金资助项目、中国空间技术研究院创新基金项目等国家及省部级科研项目20余项；获黑龙江省科技进步奖二等奖2项；发表论文100余篇，获授权国家发明专利40项。

李季蹊，哈尔滨工业大学在读硕士研究生；主要研究方向为物理层安全与空天地通信网络。

李静涛，中国空间技术研究院通信与导航卫星总体部研究员；主要研究方向为无线通信与通信卫星系统设计。