综述

空天地通信网络中物理层安全技术综述

闫富朝，刘怡良，韩帅，孟维晓
（哈尔滨工业大学，黑龙江 哈尔滨 150001）

摘　要：空天地一体化通信网络是未来无线通信的发展趋势，其固有的广播特性和广阔的覆盖区域，将导致网络通信系统面临严重的安全威胁。如何保证空天地通信网络的安全性是一个亟待解决的问题。物理层安全技术作为一种有效的安全手段，在无线通信领域受到越来越多的关注。介绍了物理层安全的基础以及空天地通信信道模型，并对物理层安全中常见的窃听编码、波束成形、人工噪声、中继协作干扰和物理层密钥加密等技术进行了介绍和总结，最后提出了空天地通信网络中物理层安全面临的挑战和未来的发展趋势。

关键词：空天地通信网络；物理层安全；窃听编码；波束成形和人工噪声；中继协作干扰；物理层密钥加密
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020263

A survey of physical layer security in space-air-ground communication and networks

YAN Fuchao, LIU Yiliang, HAN Shuai, MENG Weixiao
Harbin Institute of Technology, Harbin 150001, China

Abstract: Space-air-ground communication and networks are the trend of wireless communication in the future. Because of its inherent broadcast nature and wide coverage, its communication and network systems will face serious security problems. How to ensure the security of space-air-ground communication and networks is an urgent problem to be solved. As an effective means of security, physical layer security technology has attracted more and more attentions. The basis of physical layer security and the channel model of space-air-ground communication and networks were introduced, and then the common technologies in physical layer security were introduced and summarized, such as wiretap coding, beamforming and artificial noise, relay cooperation interference and physical layer key generation, finally the challenges and future development trend of physical layer security in space-air-ground communication and networks were proposed.

Key words: air-space-ground communication and networks, physical layer security, wiretap coding, beamforming and artificial noise, relay cooperation interference, physical layer key generation

收稿日期：2020−05−19；**修回日期**：2020−08−27
基金项目：国家自然科学基金资助项目（No.61771169）；黑龙江省自然科学基金资助项目（No.ZD2017013）
Foundation Items: The National Natural Science Foundation of China (No. 61771169), The Natural Science Foundation of Heilongjiang Province of China (No. ZD2017013)

1 引言

1.1 研究的背景和意义

近年来，随着科学技术的发展，无线通信技术已经得到了飞速的发展，为政府、科研和商业都带来技术性的革新，也为人们的生活提供了极大的便利。蓝牙、卫星、射频识别（radio frequency identification，RFID）、无线局域网（wireless local area network，WLAN）、5G、卫星通信等无线通信技术应用在国民经济和日常生活的方方面面。

虽然陆地网络已经得到了长足的发展，但由于地面网络基础设施的局限性，对于一些边远和环境恶劣地区网络信号仍难以覆盖，空天网络可以有效填补这些空白。空天地一体化已经成为未来无线通信网络的发展趋势，因其固有的广播特性和巨大的覆盖特性，必将带来严重的无线通信安全问题。因为无线通信系统的传输媒介是能够在自由空间中传播的电磁波，并且无线信道具有的开放性、无线终端具有的移动性以及无线网络结构的不稳定性等，导致在无线通信过程中存在许多诸如被窃听、干扰、黑客攻击、非法接入等安全性问题。相对于地面通信网络，空天通信的物理环境更加恶劣。且卫星等移动节点处理能力更弱，网络拓扑结构动态变化更快，使空天地一体化通信网络更容易遭受攻击，这将给国家的通信和导航等领域带来严重的威胁。

2016 年，我国颁布了《中华人民共和国网络安全法》，从国家层面强调了网络安全的重要性。同时“强化信息安全保障”是我国列入“十三五”规划重点发展的战略性新型产业。在学术界，国内许多高等院校如清华大学、北京航空航天大学和东南大学等也纷纷成立网络空间安全学院。网络空间安全已经受到了越来越多的关注。

传统的安全通信技术主要是基于密钥体系，是在通信网络的上层实现的。然而，在一些网络结构中密钥的管理和分发将变得非常复杂或者难以实现，例如，分布式系统不存在中心节点。另外，在物联网中存在很多简单的设备，无法实现加密和解密的功能。并且，随着计算机计算性能的不断提高，破解密钥所需要的成本越来越低。在这样的背景下，新型安全通信技术的研究变得至关重要。物理层安全则利用无线信道的特性以及物理层技术实现无线通信的保密传输[1]，可以作为传统加密技术的一种有效补充，形成从物理层到应用层全方位的信息安全保护。物理层安全技术不依赖运算复杂度，即使对方有较强的计算能力也无法损害无线传输的安全性；并且不依赖中央控制系统对密钥进行分发和管理，对设备要求不是特别高，适用于未来的无线通信系统。随着物理层安全在信息安全领域中地位和作用的逐渐提升，物理层安全的研究已经成为了当前无线通信领域中的研究热点。物理层安全有望为空天地通信网络的安全性和保密性构筑一层坚固的屏障。

1.2 空天地通信网络的架构和安全性挑战

空天地一体化通信网络是以地面网络为依托、天基网络为扩展，采用统一的技术架构、体制和规范，主要由天基骨干网、天基接入网和地面骨干网 3 部分组成[2]，空天地通信网络模型如图 1 所示。

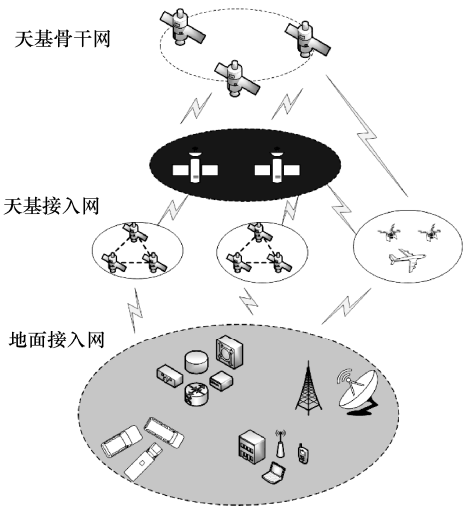

图 1 空天地通信网络模型

天基骨干网一般由深空探测卫星和遥感卫星等多种卫星以及其他接近地球同步轨道的天基骨干节点组成。天基骨干网主要由一些高轨卫星组成，具有一定的计算和存储能力，可以直接与地面设备通信。对于高轨卫星来说，由于距离地球太远，往返时间长，时延较大。天基接入网一般由宽带卫星接入网、移动卫星接入网、低轨卫星接入网和近地接入网组成。天基接入网主要由中轨卫星和低轨卫星组成，时延相对较小，主要是利用星间链路实现空间物联网，天基骨干网和地面骨干网之间的数据交换和中继任务。地面骨干网一般由移动接入网、固定接入网、移动网和地面基站组成，主要负责实现各种网络之间的互联互通。基于地面的网络具有巨大的计算能力和存储空间，可以处理卫星传回的数据和地面其他子网传输的数据。

尽管空天地一体化通信网络已经被提出多年，但目前仍有较多的技术障碍，比如动态网络拓扑的设计、卫星之间的协同传输和频谱的干扰抑制等，并且近年来空天地一体化网络的安全性问题也受到了越来越多的关注。由于在空天地一体化网络中，数据是通过无线链路直接传输的，具有较强的开放性，并且卫星网络的拓扑结构是动态的，使得空天地一体化网络更容易受到攻击，遭受窃听，使国家安全受到威胁。空天地通信网络需要同时将地面和空间的各种移动节点连接到一起，具有空间跨度大、时延较长和反馈链路少等特点，并且卫星与卫星之间和卫星与地面的之间的通信环境复杂，再加上时空约束和空间资源的受限，使得空天地通信网络的安全性面临巨大的挑战[1]。相对于传统的保密技术，物理层安全技术通过利用保密编码、协作干扰、波束成形和人工噪声、物理层密钥技术等可以有效加强空天地通信网络的安全性和保密性。

2　物理层安全基础

2.1　物理层安全技术的发展

保密通信是 1949 年由 Shannon 首次提出的，他从信息论的角度对保密通信进行了研究[3]。然而，其提出的密钥生成和管理在实际应用中十分困难。1975 年，Wyner 提出了窃听信道模型[4]（如图 2 所示），利用主信道和窃听信道之间的差异，在物理层实现完全保密，由此揭开了物理层安全的面纱。

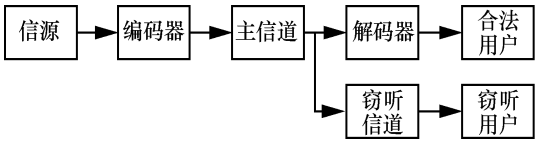

图 2　窃听信道模型

物理层安全的研究一般分为两个方面：一个是从信息论的角度出发，研究系统的保密能力，给出一个系统的框架；另一个是从信号处理的角度出发，通过优化信号处理技术，实现系统的安全策略设计。参考文献[5]关于物理层安全的研究，在国内外有很多文献都进行了系统的描述，如参考文献[6-10]就针对不同的信道类型、通信场景和信道状态信息等，对系统可实现的保密性能进行了研究。现在的物理层安全方案仍还有许多不完善的地方，比如大部分物理层安全方案都基于窃听信道，与合法信道之间有较大差异，合法信道和窃听信道的信道状态全部已知或部分已知等条件，然而现实情况往往不满足这些条件，因此它离实际应用还有较长的路要走。

本文将从空天地一体化网络的背景出发，系统全面地介绍现存的适用于空天地通信网络的物理层安全技术，对它们的优缺点进行分析，并对未来的发展趋势作出预测，为其他研究人员提供参考。

2.2　空天地通信网络的信道模型

对于无线通信系统，信道和信道的传播特性

是它的重要组成部分，也在很大程度上决定着通信系统的性能。对于空天地通信网络，其信道模型可以分为天地、空地和地地 3 部分。其中，地地之间的信道模型研究已经比较成熟，在此不再进行赘述。

天地信道模型主要指星地之间的链路，星地链路的常用频段包括 VHF、UHF、L、C 和 K 等频段。不同的频段对应的卫星业务也不同，具体的频段和业务分配见表 1。

表 1　卫星常用频段

频段	频率范围/GHz	卫星业务
VHF	0.1～0.3	气象卫星等
UHF	0.3～1.0	导航、定位和气象卫星等
L	1.0～2.0	卫星定位、卫星通信等
S	2.0～4.0	卫星通信、气象雷达等
C	4.0～8.0	卫星固定业务等
X	8.0～12.0	雷达和卫星通信等
Ku	12.0～18.0	卫星固定业务及直播星业务等
K	18.0～27.0	卫星电视和广播等
Ka	27.0～40.0	高速卫星、DTH 等

相比于陆地之间的信道模型，星地之间的链路质量会受大雨、大雾和倾角等的影响，同时在卫星通信中经常会使用多波束技术，所以在进行信道建模时需要同时考虑卫星波束和路径损耗两方面。在此，设 f_k 表示地面站和第 k 个波束之间的信道系数，表示为[11]：

$$f_k = h_k C_k \tag{1}$$

其中，h_k 表示随机阴影系数，通常用复合衰落分布进行模拟，常见的数学模型有很多，但 SR 模型被认为是最符合星地链路特点的模型，它在不同的频带都得到了很好的应用[12]。C_k 表示传播损耗，包括自由空间传播损耗和方向图损耗。

空地信道模型主要指空中飞行物（如无人机等）与地面基站之间的链路。在关于无人机与地地面之间的信道模型也有很多，其中 3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）在 2017 年提出的 GBS-UAV（ground base station-unmanned aerial vehicle，地面基站与无人机）信道模型考虑因素最全面也最权威，本小节主要介绍该信道模型。对于无人机与地面之间的信道模型，最重要的便是直射概率的确定，对于不同的直射概率，其相应的阴影衰落和路径损耗模型也不同。同时空地信道模型也与工作频段有关，工作频段不同，相应的路径损耗也不同，频段越高，路径损耗相应越大；工作频段的不同，也会导致多普勒频移的不同，相应的信道衰落模型也会不同，在此不再进行具体的分析。

对于直射概率，主要与地面基站和无人机之间的空间距离 $d_{2\text{-D}}$ 和无人机高度 H_{U} 有关[13]。当 H_{U} 低于阈值 H_1 时，该概率模型与地面通信概率模型相同，当 H_{U} 高于阈值 H_2 时，可认为概率是 1。当 H_{U} 处于两个阀值之间时，该概率就是 d_{2-D} 和 H_{U} 的函数。具体表达式为：

$$P_{\text{Los}} = \begin{cases} P_{\text{Los,ter}}, & H_{\text{U}} < H_1 \\ P_{\text{Los,U}}(d_{2-\text{D}}, H_{\text{U}}), & H_1 \leqslant H_{\text{U}} \leqslant H_2 \\ 1, & H_2 < H_{\text{U}} \end{cases} \tag{2}$$

其中，$P_{\text{Los,ter}}$ 是常规地面通信的直射概率模型，具体如参考文献 [14] 中表 7.4.2 所示。而 $P_{\text{Los,U}}(d_{2-\text{D}}, H_{\text{U}})$ 表示为：

$$P_{\text{Los,U}}(d_{2\text{-D}}, H_{\text{U}}) = \begin{cases} 1 & d_{2\text{-D}} \leqslant d_1 \\ \dfrac{d_1}{d_{2-\text{D}}} + \exp\left(\dfrac{-d_2 - D}{p_1}\right)\left(1 - \dfrac{d_1}{d_{2-\text{D}}}\right) & d_{2\text{-D}} \geqslant d_1 \end{cases} \tag{3}$$

其中，p_1 和 d_1 由 H_{U} 的对数增长函数给出，H_1 和 H_2 则根据不同的应用场景设置不同的阀值。

2.3　物理层安全技术的评价指标

对于安全传输设计，性能指标的选择是非常关键的。在物理层安全设计中，由于性能要求的不同，通常会出现以下情况。

- 安全传输策略的传输有效性，即通过可实

现的保密率/容量来评估。

- 安全传输策略的可靠性，用保密中断概率/容量来衡量。
- 安全传输策略中的能量保密效率，它关注用单位能量传输的秘密比特的数量或发送一个秘密比特所需的能量消耗。

为了研究上述问题，系统设计中通常采用保密率/容量、保密中断概率/容量、能量保密效率等评估提出的安全传输策略的可实现性能。更具体地说，这些性能指标通常作为不同应用场景中系统设计的优化目标[3]。

保密容量：保密容量指的是可以同时保证合法用户之间进行可靠通信又能对窃听者实现完全保密的情况下所能实现的最大通信速率。在加性高斯白噪声信道下，保密容量可以保密为主信道和窃听信道之间的容量差。具体计算式为：

$$C_s = \max[I(X,Y_{\mathrm{B}}) - I(X,Y_{\mathrm{E}})]^{+} \tag{4}$$

其中，$[X]^{+} = \max(X,0)$，X 表示源节点处的信道输入，Y_{B} 和 Y_{E} 分别表示目标节点和窃听节点的信道输出，I 表示信道输入与输出之间的互信息量。

保密速率：保密容量难以获得，研究中通常采用保密速率这一指标。保密速率指的是主信道和窃听信道之间的数据传输速率差，表示为：

$$R = [C_{\mathrm{B}} - C_{\mathrm{E}}]^{+} \tag{5}$$

其中，C_{B} 表示主信道的香农信道容量，也是主信道能够达到的最大信息速率，C_{E} 表示窃听信道的香农信道容量。

遍历保密容量：保密容量和保密速率通常在某一固定信道下使用，不考虑信道衰落的影响。为了刻画信道时变特性的影响，就需要利用遍历保密容量来进行度量，它是指在衰落信道下进行保密传输的平均能力，具体计算式如式（6）：

$$C_s = \max \boldsymbol{E}[C_{\mathrm{B}} - C_{\mathrm{E}}]^{+} \tag{6}$$

其中，$\boldsymbol{E}[\bullet]$ 表示信息变量的平均值，C_{B} 和 C_{E} 分别表示主信道和窃听信道的信道容量。

保密中断概率：对于时延受限的系统来说，在多个信道状态下进行编码是不可行的，它会导致更大的时延，此时就需要用保密中断概率进行安全性度量。保密中断概率指的是系统当前的保密速率低于设置的门限值的概率，可以由式（7）进行计算：

$$R_{\mathrm{out}}(R_t) = \Pr\{C_s < R_t\} \tag{7}$$

其中，C_s 表示当前的保密速率，R_t 表示保密数据的传输率门限值。

保密区域：保密区域是从大尺度衰落信道的角度来度量安全性能的，它指的是保密容量为正的几何区域。假设（x,y）是窃听者的坐标，保密区域可以表示为一组坐标：

$$R_{\mathrm{region}} = \{(x,y), C_{\mathrm{E}}(x,y) < C_{\mathrm{m}}\} \tag{8}$$

其中，$C_{\mathrm{E}}(x,y)$ 表示坐标为 (x,y) 的窃听者处的信道容量，C_{m} 表示主信道容量。

能量保密效率：当系统同时考虑安全性能和能耗限制时，设计能量利用效率高的通信方案就很有必要。此时能量保密效率便是一种常用的衡量指标，它是指单位功率所能发送的保密信息比特数，如式（9）所示：

$$\eta_{\mathrm{SEE}} = \frac{R_{\mathrm{s}}}{E_{\mathrm{t}}} \tag{9}$$

其中，R_{s} 表示主信道信息传输速率，E_{t} 表示系统消耗的总能量。

3　空天地网络下的物理层安全技术

空天地通信网络具有覆盖范围大、上下跨度广、空间资源受限以及功率约束大等特点，对物理层安全技术的需求相比地面通信有所不同。物理层安全的主要策略是降低窃听者处的信干噪比，常见的技术有窃听编码、波束成形、人工噪声和中继协作干扰等，近几年又出现了跨层协作的物理层安全研究方案，利用主信道物理层资源产生密钥实现保密传输。本节将对以下技术进行

具体的介绍，并对其局限性进行分析。

3.1 物理层安全编码

在 Shannon 建立了信息论安全的基本概念之后，就有许多学者开始研究安全信道编码。Wyner 和其他研究人员也证明了随机信道编码的存在，随着数据块长度趋于无穷，随机信道编码既能够保证可靠性又能够保证一致性[15]。

参考文献[16]首次提出了使用陪集来设计安全编码。参考文献[17]从信息论的角度研究了编码极限和针对窃听信道的编码方法，并提出利用 LDPC（low density parity check code，低密度奇偶校验码）实现系统保密是可行的。参考文献[18]提出了一种新的可以获得系统保密容量的编码结构，在与参考文献[17]相同的信道条件下，可以实现更好的保密性能。参考文献[19]研究了在相同情况下，在最大似然译码情况下 LDPC 码的保密性能，并证明了在无记忆二进制对称信道和任意速率的最大似然译码情况下，可以通过对任意小速率的 LDPC 码进行删减来获得系统的保密容量。对于高斯窃听信道，在参考文献[20]中提出了一种基于 LDPC 编码的使用编码方案，该方案适用于有限长数据，通过利用信道的统计特性来改善系统的保密性能。参考文献[21]构造了一种码长较小的不规则 LDPC 码，使其性能接近理论极限。

近几年，极化码（也称 polar 码）也被用作物理层安全编码来提高系统的保密性。Mahdavifar 和 Vardy[22]利用 polar 码构造了一种能够广泛地在窃听信道模型中实现系统保密传输的编码方案。该方案适用于所有主信道和窃听信道都是二进制对称信道并且主信道优于窃听信道的情况。除了基于 LDPC 和 polar 码的安全编码方案外，也有基于其他编码的保密方案。如参考文献[23]研究了卷积码和 turbo 码在高斯窃听信道中使用随机编码方法的方案。上述编码方案都是基于地面网络，参考文献[24]从卫星信道的角度回顾了窃听编码的概念，介绍了窃听编码的一般结构，并分析了它对典型卫星信道的适用性。

上述的研究中大多数物理层安全编码方案大多是基于有限的数据块长度并且需要保证零差错传输，并且大都针对地面网络。而在实际的通信网络中，并不需要这么严格的保密，并且上述的编码方案都比较复杂，在实际通信系统中应用还比较困难，同时针对天基骨干网络的编码方案也亟待开发。

3.2 波束成形和人工噪声

波束成形和人工噪声都属于信号处理技术，是当前物理层安全研究中比较有潜力的技术，对于提高系统的保密速率、降低系统的中断概率和能耗等有很大优势。在不考虑安全性的传统多天线系统中，波束成形技术不仅能够获得与空时编码相同的分集增益，还能获得更高的编码增益。在物理层安全通信中，波束成形技术也是一种非常重要的技术，利用空间自由度使信号传输具有指向性，增强合法用户的接收信号质量，从而获得保密容量实现安全通信[25]。其核心思想是通过对各发射天线的信号的相位的调节，使合法接收者方向信号强度变大，非法接收者信号强度变小。但波束成形是假设系统准确地已知窃听者的瞬时 CSI（channel status information，信道状态信息）。然而在实际的系统中，系统很难已知被动窃听者的瞬时 CSI，甚至可能完全未知窃听者的 CSI。然而不准确的瞬时 CSI 会导致波束成形向量的设计产生误差，从而导致系统的保密性能下降。人工噪声技术可以在未知窃听者的瞬时 CSI 的情况下，在不影响合法接收者信道质量的前提下，对窃听者进行干扰。基于零空间的人工噪声的原理即发送有用信息的同时，分出一部分功率发送人工噪声，利用空间自由来设计人工噪声，使人工噪声存在于发送端与合法接收者之间主信道的零空间内，来保证合法接收者的接收不受影响，而非法窃听端则由于人工噪声的影响，信号质量变

得很差，接收信噪比急剧下降，从而提高整个系统的保密速率。

参考文献[25]在卫星网络中采用了动态的波束成形技术，使得在卫星的边带处不能获得信息，从而实现了系统的保密性。参考文献[26]研究了分散在多个波束中的固定合法接收机的物理层安全技术，每个波束可能被多个窃听者包围。在窃听者信道状态信息完全可知时，设计了一种结合半正定松弛和基于梯度的迭代算法，在满足合法用户保密速率限制的同时，最小化卫星上波束的总发射功率。参考文献[27]研究了多波束卫星通信系统中的物理层安全性。提出了迫零和漏信噪比两种波束成形算法，并利用仿真结果验证了两种方法的有效性，在满足卫星的发射功率限制下，可以最大化系统的保密速率。参考文献[28]研究了多波束卫星网络中的物理层安全技术，提出了波束成形和功率控制下多波束卫星物理层安全传输的策略。参考文献[29]首次提出了利用多天线在主信道的零空间产生人工噪声的方法。参考文献[30]讨论了位于零空间的人工噪声在不影响合法接收者接收的情况下，可以大大降低窃听者处接收的信号质量，从而提高系统的保密性。参考文献[31]研究了慢衰落系统中人工噪声辅助的多天线安全传输的设计，重点讨论了传输功率分配和窃听码的速率参数，并考虑了具有不同复杂度的情况，一种是固定传输，另一种是对接收者的瞬时信道状态进行反馈并自适应地进行调整。参考文献[32]重点研究了在不限制窃听者天线数量的情况下的人工噪声方案并且文献还对保密速率的上下限做了推导。参考文献[33]提出了一种基于 Wishart 矩阵的编码方案，在矩阵有序特征值的 S 个最强本征子信道中对消息进行编码，而人工噪声在剩余的空间中生成。与现有的方案相比，该文献中提出的人工噪声方案的保密能力可以提高约 20%。

现存的波束成形或人工噪声方案都需要完美已知系统的全部信道状态信息或者主信道的信道状态信息，而在实际的系统中由于信道估计带来的误差而很难满足该条件，因而会影响系统的保密性能。同时人工噪声方案大多都基于发射端天线数量大于窃听者天线数量，而卫星通信系统中会受天线数量的约束。同时，在卫星通信网络中，由于星地之间的距离过大，合法接收者和窃听者之间的距离与星地距离相比往往可以忽略，因此主信道和窃听信道之间的差异性很小，这种情况下现存的人工噪声方案往往都会失效。下一步，需要根据以上因素设计更加适合空天地通信网络的波束成形和人工噪声方案。

3.3　中继协作干扰

在卫星网络中，卫星和地面用户之间的直射路径可能由于较大的障碍物（如高山等）以及阴影遮蔽效应等因素而变得不可用，从而限制了卫星和地面目的地之间直射路径的信息传输。当卫星仰角较低或地面用户为室内用户时，障碍物引起的掩蔽效应更为严重[34]。为了克服这一问题，引入了一种称为 HSTRN[35-37]的新架构，通过充分利用地面中继站带来的空间分集，卫星网络可以与现有地面网络很好地集成。在这种架构下，卫星发射信号可以在地面中继站的协助下可靠地转发给地面用户。地面中继可以是单天线或多天线，也可以是多个中继合作通信[38]。同时，中继还可以用来增强信息传输的安全性，中继协作干扰通信模型如图 3 所示，便是中继协作干扰的通信模型。在该模型下，中继节点通常有两种方法来增强系统的安全性；转发加密信息或发送干扰信号来迷惑窃听者。参考文献[39]在单中继、单用户和单窃听者存在的场景下调查了 HSTRN 的保密能力，通过两级波束成形方案，得到了系统的最优保密容量表达式。

由于卫星覆盖面积大，为了进一步提高 HSTRN 架构的空间分集性能，多中继受到了越来越多的关注。Yan 等[40]设计了一种单用户多中继

网络在多个窃听器存在下的安全传输方案，其中中继波束形成矢量和干扰信号矢量被联合优化以最大化系统的保密速率。参考文献[41]中的安全传输方案分为两个阶段，第一阶段是在合法接收者处使用多载波来发送人工噪声，使得窃听者的信道急剧恶化，然后在第二阶段，地面基站利用波束成形技术将其接收到的卫星信号转发给合法用户。参考文献[42]考虑了单用户多中继网络在一个窃听者存在下的情况，在不同信道状态信息需求的条件下基于放大转发中继的最优选择方案。参考文献[43]讨论了在理想的信道状态条件下，基于解码转发的单用户多中继网络中的最优中继选择方案。参考文献[44]考虑了窃听信道的瞬时信道状态信息不可用的情况下的安全传输方案。通过采用单中继和多中继选择方案，在窃听者可以同时截获来自卫星和多个中继的信号情况下，通过保密中断概率来评价系统的保密性能。

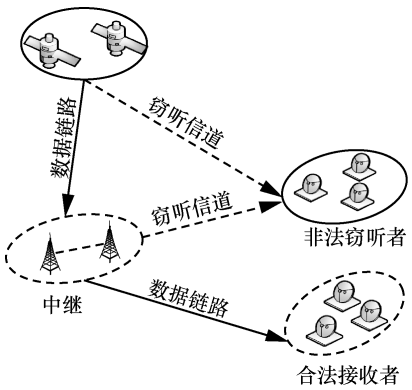

图 3　中继协作干扰通信模型

进一步地，HSTRN 又扩展了多用户多中继的情况，以更好地提高系统的保密性能。参考文献[45]研究了多中继和多用户之间的联合机会中继选择和用户调度方案，以提高 HSTRN 的系统安全性，同时考虑了串通和非串通两种窃听情况。在参考文献[46]中，对多个窃听者存在的多用户多中继通信网络进行了全面的保密性能分析，考虑了两种不同的窃听场景，即合作窃听者和非合作窃听者，提出了一个机会用户中继选择准则，然后分别利用放大转发和解码转发中继协议推导出了系统保密中断概率的精确表达式。参考文献[47]调查了卫星通信中合作中继的使用情况，将系统中的中继节点分为协作转发组和协作干扰组，分别提高主信道质量和降低窃听信道质量，从而降低系统的保密中断概率，提高系统的保密性能。

中继协作干扰技术常与波束成形技术以及人工噪声技术相结合，在中继节点进行信号重传的同时发送干扰，原理简单并且容易实现。但中继协作干扰可能会导致额外的开销，此时又有学者提出了不可信中继的概念，在尽量减少功率消耗的情况下增强系统的保密性，但随之带来的是中继选择方案的复杂性增大，将来还有待继续优化。

3.4　基于物理层的密钥加密技术

现有的物理层安全传输策略主要有两类，一类是上述的窃听编码、波束成形、人工噪声和中继协作干扰等技术，另一类便是基于物理层的密钥加密方法，主要包括基于无线信道特征的密钥提取、物理层符号加密等方法。相比于传统的密钥加密方法，由于物理层密钥加密技术利用的是信道特征等信息，具有唯一性，不会因窃听端计算能力的提高而被破解，因此这种跨层的保密技术也受到越来越多人的关注[48]。根据 Jakes 均匀散射模型，当合法接收者与窃听者之间的间隔在超过大约半个波长的距离之后，主信道与窃听信道的特性便是不相关的。基于物理层的密钥加密技术也正是利用了这种独特的信道衰落特性，使得窃听者很难正确破解密钥实现窃听。

物理层密钥加密技术主要是利用无线信道的时变性，现有的研究主要针对 RSS（receive signal strength，接收信号强度）、CSI、OFDM（orthogonal frequency division multiplexing，正交频分复用）中的信道频率响应和载波频率偏移等特征进行提

取生成密钥。密钥生成的基本步骤可以概括为以下 4 个步骤：

（1）在通信双方对信道进行相关性测量；

（2）提取信道特征作为公共随机变量；

（3）对信道进行量化生成随机密钥；

（4）对信道特征进行优化使密钥适合传输。

在时域，物理层加密技术可以利用信道由于衰落、干扰和色散等引起的变化来提取密钥，并且时域信道互易性较强，不容易失配。参考文献[49]提出了一种利用信道短期互易性来保护信息的技术，该文献利用信道衰落系数的相位来作为密钥，同时该技术还可以用于用户之间的密钥协商。参考文献[50]通过优化发射阵列，使通信信道中产生更多的反射，从而提取密钥。参考文献[51]利用 ARQ（automatic repeat request，自动重传请求）的一位反馈消息来生成密钥。参考文献[52]提出了一种利用 RSS 的单次测量来提取密钥的自适应技术，同时作者还通过优化密钥来增强密钥之间的匹配程度，同时还在真实的通信环境中对信道进行了测量，以展示方案的有效性。与基于时域信道变化的密钥提取类似，频域也可以用于密钥的生成。参考文献[53]研究了在 OFDM 无线通信系统中利用信道的时变频率响应和信道相位来生成密钥。参考文献[54]提出了一种基于 OFDM 子载波和预编码矩阵索引的密钥生成方法。参考文献[55]提出了一种快速可靠的基于 RSS 的 OFDM 系统密钥生成方法，利用 Wi-Fi 板卡在室内环境下从 OFDM 多个子载波提取信道状态信息生成了密钥，证明了 OFDM 系统用于密钥生成的有效性和可行性。

物理层密钥加密技术相比于传统的加密技术，增强了密钥的随机性，减少了密钥分配、共享、存储和管理等问题。然而，物理层密钥加密技术并不能实现完美保密，其密钥长度和有效性会受到信道变化的限制，同时不准确的信道估计和信道互易失配也会使得生成的密钥不适合通信双方，从而降低合法接收者处的接收信号质量，另外当信道散射性差，没有太多随机性变化时，物理层密钥加密技术就会失去意义，这些还有待解决。除了上述的物理层安全技术，广义的物理层安全技术还包括物理层认证、隐蔽通信和攻击检测等，这些技术一起为物理层安全提供了保障。

4　未来愿景与挑战

21 世纪是信息的时代，人们对信息的需求越来越大，对信息化服务的要求也越来越高。空天地一体化通信网络就是人们对未来通信模式的一个美好愿景，将空天地 3 个维度的所有目标都连接起来，实现真正的万物互联，为用户提供全球的无缝连接服务。与之而来的，通信网络的模型也将更加复杂，连接节点的增多，也给系统带来了更大的安全风险。

4.1　天地安全

目前，对于天地通信来说，主要是利用高轨卫星进行组网通信，比如我国自主研制的“天通一号”。然而高轨卫星在中低纬度的通信角度较小，在南北极存在盲点。并且高轨卫星的时延较大，在体积、功耗和容量方面也有较大的限制。于是，低轨卫星组网受到了越来越多的关注。比如近几年国外提出的 OneWeb 卫星星座、SpaceX 卫星系统以及国内提出的虹云工程、鸿雁星座等，都是利用几百颗甚至上千或者上万颗低轨卫星进行组网，来提供高速通信服务，实现全球无缝覆盖。因此寻找低轨卫星的安全通信的方法迫在眉睫。尤其是低轨卫星的星座相对于地球具有很高的移动速度，卫星网络拓扑是时变的，会随着卫星轨道的变化而变化，这给卫星物理层安全通信的设计带来了不小的挑战。同时，动态低轨卫星网络对角度的敏感性，主信道的信号质量变化频率高，窃听链路获得比主信道更高的信号质量的可能性会加大。因此设计角度敏感性约束的物理层安全通信手段是低轨卫星网

络之间以及与地面网络之间的研究的重点。并且，由于低轨卫星之间存在相对运动，会引入多普勒频移，对安全通信性能造成影响，这对卫星的信道接入、路由方案、卫星的位置和间隔等提出了更高要求。低轨卫星互联网正在蓬勃发展，未来将为空天地通信网络的实现提供强有力的支撑。

4.2 空地安全

对于空地通信来说，目前主要还是利用无人机作为移动基站来进行组网，作为陆地和卫星网络的有效补充，为用户提供全面有效的服务。然而，大部分方案还是将陆地、空地和卫星网络视为 3 个独立的网络，未来将三者联合起来进行协同传输将成为一个大趋势。但同时，将空、天、地上的移动节点连接起来，构成一个 3 层的异构网络也会导致网络拓扑结构异常复杂，并且不断变化，很容易就会受到攻击而造成网络瘫痪。并且 3 层网络之间的频谱资源，传输协议也可能因为不统一而互相干扰，因此商定一个统一的安全传输协议也迫在迫在眉睫。另外，将无人机应用于海洋通信的场景也受到了越来越多的关注。在近海，无人机可以和陆地网络配合；在远洋，无人机可以和卫星通信一起，形成混合网络，从而有效满足海洋中移动船舶的通信需求。但无人机轨迹的优化以及与海洋船只的配合，还有待研究。并且，海洋环境恶劣，很容易受到电磁波干扰，如何保障无人机通信在海洋网络中的安全也值得关注。尽管无人机灵活的网络拓扑结构等特性，使得它更容易受到攻击，但同时如果利用好无人机自身的特点，将无人机通信与现有的安全技术如人工噪声，中继协作干扰等有效结合起来，对于增强系统的保密性也将有很大帮助。

4.3 物理层安全技术面临的挑战和未来趋势

物理层安全作为一种有效的增强系统保密性的技术，也受到了越来越多的关注。本文介绍了现存的几种主要的物理层安全技术，包括窃听编码、波束成形与人工噪声、中继协作干扰和物理层密钥加密技术等。然而，现存的物理层安全技术还是面临很大的挑战，比如现存的大多数物理层安全研究方案都基于系统的信道状态信息完美可知、主信道和窃听信道要有较大的差异性、信道特征的变化要比较大等，而这些条件在实际中很难满足，如何克服这些挑战，在未来还有待继续深入研究。

除了上述的一些物理层安全技术，以下的物理层安全研究方向也值得关注：一是跨层安全技术，将物理层安全与经典密码学结合，从安全网络框架、安全编码方案、安全网络协议和混合加密算法等方面给出一个完整的安全解决方案；二是将安全性、可靠性和网络吞吐量联合优化，现存的研究方案大多将三者分开进行考虑，在未来可以将三者进行统一考虑，根据不同的场景和性能需求进行折中，以带来更好的用户体验；三是将窃听编码、波束成形和人工噪声以及中继协作干扰等物理层安全传输策略进行联合考虑，通过统一的资源调度，在能耗消耗尽可能少的情况下实现更强的保密性能。

尽管关于物理层安全的理论研究已经有很多，但物理层安全技术离真正的实现还有很长的路要走。现有网络框架适用性带来的障碍、底层空中接口的可扩展性、网络资源的限制以及认知无线电、物联网、高速移动网络等都给物理层安全技术带来了巨大的挑战。未来需要更多地去关注这些实际问题，推动物理层安全技术的实现，打造一个安全、高效、便捷的通信网络。

5 结束语

空天地一体化通信网络作为通信网络未来的发展趋势，受到了国家越来越多的重视。然而，由于其覆盖面积广和连接节点众多等特点，必然

会带来很多的安全性问题。物理层安全技术相比传统加密技术，不受计算机计算能力的约束，利用无线信道本身的特征来增强系统的保密性，具有广阔的应用前景。

参考文献：

[1] 韩帅, 台祥雪, 孟维晓. 空天地通信网络的物理层安全系统模型与关键技术[J]. 电信科学, 2018, 34(3): 23-31.
HAN S, TAI X X, MENG W X. Physical layer security for the air-space-ground communication networks[J]. Telecommunications Science, 2018, 34(3): 23-31.

[2] LI B, FEI Z S, CAI Q, et al. Physical-layer security in space information networks: a survey[J]. IEEE Internet of things journal, 2020, 7(1): 33-52.

[3] SHANNON C E, Communication theory of secrecy systems[J]. Bell System Technology Journal, 1949, 28(4): 656-715.

[4] WYNER A D. The wire-tap channel[J]. Bell System Technology Journal, 1975, 54(8): 1355-1387.

[5] 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): 1878-1910.

[6] MUKHERJEE A, FAKOORIAN S A A , HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550-1573.

[7] LIU Y, CHEN H H, WANG L. Physical layer security for next generation wireless networks: theories, technologies, and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 347-376.

[8] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: Technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[9] POOR H V, SCHAEFER R F. Wireless physical layer security[J]. Proceedings of the National Academy of Sciences of the United States of America, 2017, 114(1): 19-26.

[10] BLOCH M, BARROS J. Physical-layer security: from information theory to security engineering[D]. Cambridge: Cambridge University, 2008.

[11] GUO K, AN K, ZHANG B, et al. Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling[J]. IEEE Access, 2018, 6(1): 55815-55827.

[12] ABDI A, LAU W C, ALUINI M S, et al. A new simple model for land mobile satellite channels: First- and second-order statistics[J]. IEEE Transactions on Wireless Communications, 2003, 2(3): 519-528.

[13] ZENG Y, WU Q Q, ZHANG R. Accessing from the sky: a tutorial on UAV communications for 5G and beyond[J]. Proceedings of the IEEE, 2019, 107(12): 2327-2375.

[14] 3GPP. Study on channel model for frequencies from 0.5 to 100 GHz, document: TR 38.901 [S]. 2017.

[15] HAMAMREH J M, FURQAN H M, ARSLAN H. Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1773-1828.

[16] OZAROW L H, WYNER A D. Wire-tap channel II[J]. Bell Syst. Tech. J, 1984, 63(10): 2135-2157.

[17] THANGARAJ A, DIHIDAR S, ALDERBANK A R, et al. Applications of LDPC codes to the wiretap channel[J]. IEEE Transactions of Information Theory, 2007, 53(8): 2933-2945.

[18] LIU R, LIANG Y, POOR H V, et al. Secure nested codes for type II wiretap channels[C]//Proceedings of IEEE Information Theory Workshop. Piscataway: IEEE Press, 337–342.

[19] HSU C H , ANASTASOPOULAS A. Capacity achieving LDPC codes through puncturing[J]. IEEE Transactions of Information Theory, 2008, 54(10): 4698-4706.

[20] KLINC D, HA J, MCLAUGHLIN S W, et al. LDPC codes for the Gaussian wiretap channel[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 532-540.

[21] BALDI M, RICCIUTELLI G, MATURO N, et al. Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel[C]//Proceedings of IEEE International Conference on Communications Workshop (ICCW). Piscataway: IEEE Press, 2015: 435–440.

[22] MAHDAVIFAR H, VARDY A. Achieving the secrecy capacity of wiretap channels using polar codes[J]. IEEE Transactions of Information Theory, 2011, 57(10): 6428-6443.

[23] NOORAIEPOUR A, DUMAN T M. Randomized convolutional codes for the wiretap channel[J]. IEEE Transactions on Wireless Communications, 2017, 65(8): 3442-3452.

[24] ÁNGELES V C, HAYASHI M. Information-theoretic physical layer security for satellite channels[C]//Proceedings of Aerospace Conference. Piscataway: IEEE Press, 2017: 1-14.

[25] 谢骐宇. 多波束卫星通信系统中的物理层安全传输算法设计与实现[D]. 长沙: 湖南大学, 2018.
XIE Q Y. Design and implementation of physical layer secure transmission algorithm in multibeam satellite communication system[D]. Changsha: Hunan University, 2018.

[26] GAO Y, AO H, FENG Z, et al. Modeling and practise of satellite communication systems using physical layer security: a survey[C]//Proceedings of IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). Piscataway: IEEE Press, 2017: 829-832.

[27] ZHENG G, ARAPOGLOU P D, OTTERSTEN B. Physical layer security in multibeam satellite systems[J]. IEEE Transactions on Wireless Communications, 2012, 11(2): 852-863.

[28] LU W X, JIANG Y W, YIN C Y, et al. Security beamforming algorithms in multibeam satellite systems[C]//Proceedings of IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). Piscataway: IEEE Press, 2017: 1272-1277.

[29] MA D, LIU X, WANG X, et al. On the performance indexes of physical layer security for multi-beam satellite networks[C]// Proceedings of International Conference on Wireless Communications & Signal Processing. Piscataway: IEEE Press, 2015: 1-6.

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

[31] ZHANG X, ZHOU X Y, MCKAY M R. On the design of artificial-noise aided secure multi-antenna transmission in slow fading channels [J]. IEEE Transactions on Vehicular Technology, 2013, 62(5): 2017-2181.

[32] LIU S Y, HONG Y, VITERBO E. Artificial noise revisited[J]. IEEE Transactions on Information Theory, 2015, 61(7): 3901-3911.

[33] LIU Y L, CHEN H H, WANG L G. 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.

[34] BHATNAGAR M R, ARTI M K. Performance analysis of AF based hybrid satellite-terrestrial cooperative network over generalized fading channels[J]. IEEE Communication Letters, 2013, 17(10): 1912-1915.

[35] PAILLASSA B, ESCRIG B, DHAOU R, et al. Improving satellite services with cooperative communications[J]. International Journal of Satellite Communication Networks, 2011, 29(6): 479-500.

[36] ARTI M K, JAIN K. Relay selection-based hybrid satellite-terrestrial communication systems[J]. IET Communications, 2017, 11(17): 2566-2574.

[37] EVANS B. Integration of satellite and terrestrial systems in future multimedia communications[J]. IEEE Transactions on Wireless Communications, 2005, 12(5): 72-80.

[38] KUANG L, CHEN X, JIANG C, et al. Radio resource management in future terrestrial-satellite communication networks[J]. IEEE Transactions on Wireless Communications, 2017, 24(5): 81-87.

[39] AN K, LIN M, LIANG T, et al. Secure transmission in multi-antenna hybrid satellite-terrestrial relay networks in the presence of eavesdropper[C]//Proceedings of IEEE International Conference on Wireless Communications and Signal Processing (WCSP). Piscataway: IEEE Press, 2015: 1-5.

[40] YAN Y, ZHANG B, GUO D, et al. Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network[C]//Proceedings of IEEE 25th Wireless & Optical Communications Conference (WOCC). Piscataway: IEEE Press, 2016: 1-5.

[41] CHEN C, SONG C. Secure communications in hybrid cooperative satellite-terrestrial networks[C]//Proceedings of IEEE 87th Vehicular Technology Conference (VTC-Spring). Piscataway: IEEE Press, 2017: 1-5.

[42] BANKEY V, UPADHYAY P K. Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes[C]//Proceedings of IEEE 85th Vehicular Technology Conference(VTC Spring). Piscataway: IEEE Press, 2017: 1-5.

[43] CAO W, ZOU Y, YANG Z, et al. Secrecy outage probability of hybrid satellite-terrestrial relay networks[C]//Proceedings of IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2017:1-5.

[44] CAO W, ZOU Y, YANG Z, et al. Relay selection for improving physical-layer security in hybrid satellite-terrestrial relay networks[J]. IEEE Access, 2018, 6(2): 65275-65285.

[45] GUO K, AN K, ZHANG B, et al. Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling[J]. IEEE Access, 2018, 6(2): 55815-55827.

[46] 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.

[47] LIU J, WANG J, LIU W, et al. A novel cooperative physical layer security scheme for satellite downlinks[J]. Chinese Journal of Electronics, 2018, 27(4): 860-865.

[48] 邱晓英. 智能化物理层安全认证及传输技术研究[D]. 北京: 北京邮电大学, 2019.
QIU X Y. Research on intelligent physical layer security authentication and transmission technology[D]. Beijing: Beijing University of Posts and Telecommunications, 2019.

[49] KOORAPATY H, HASSAN A A and CHENNAKESHU S. Secure information transmission for mobile radio[J]. IEEE Communications Letters, 2000, 4(2): 52-55.

[50] AONO T, HIGUCHI K, OHIRA T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784.

[51] ABDALLAH Y, LATIF M A, YOUSSEF M, et al. Keys through ARQ: theory and practice[J]. IEEE Transactions Information Forensics Security, 2011, 6(3): 737-751.

[52] JANA S. On the effectiveness of secret key extraction from

wireless signal strength in real environments[C]//Proceedings of ACM MobiCom, Piscataway: IEEE Press, 2009:321-332.

[53] WANG Q, SU H, REN K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//Proceedings of IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2011: 1422-1430.

[54] WU C Y, LAN P C, YEH P C, et al. Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1687-1700.

[55] LIU H, WANG Y, YANG J, et al. Fast and practical secret key extraction by exploiting channel response[C]//Proceedings of IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2013: 3048-3056.

[作者简介]

闫富朝（1996− ），男，哈尔滨工业大学硕士生，主要研究方向为物理层安全与空天地通信网络。

刘怡良（1990− ），男，哈尔滨工业大学博士生，主要研究方向为物理层安全、车载通信安全。

韩帅（1981− ），男，博士，哈尔滨工业大学教授、博士生导师，主要研究方向为卫星通信、宽带无线通信、物理层安全和室内定位等。

孟维晓（1968− ），男，博士，哈尔滨工业大学电子与信息工程学院副院长、教授、博士生导师，主要研究方向为无线通信与网络、空天地信息传输、精确定位与无缝导航。