



专题：网络空间安全

## 空天地通信网络的物理层安全系统模型与关键技术

韩帅, 台祥雪, 孟维晓

(哈尔滨工业大学, 黑龙江 哈尔滨 150001)

**摘要:** 空天地通信网络作为无线通信的典型应用, 因其固有的广播性质和广泛的覆盖区域, 面临严重的无线通信安全问题。尤其在军用卫星通信方面, 安全通信保障要求更是至关重要, 如何实现通信的安全是一个必须要面对的问题。提出了空天地通信网络物理层安全通信的模型——协作一直连混合星地物理层安全通信系统模型。在该模型的基础上, 通过研究中继选择问题、卫星和中继的功率分配问题等进一步提升系统的安全性能, 并且以此提出了一个整体的适应空天地通信网络的保密性增强方案, 旨在为未来的空天地物理层安全提出一套技术理论框架。

**关键词:** 空天地通信网络; 物理层安全; 中继选择; 功率分配

**中图分类号:** TP393

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-0801.2018129

## Physical layer security for the air-space-ground communication networks

HAN Shuai, TAI Xiangxue, MENG Weixiao

Harbin Institute of Technology, Harbin 150001, China

**Abstract:** As a typical application of wireless communications, the air-space-ground communications networks are facing serious wireless communications security issues due to its inherent broadcast nature and wide coverage. Especially in the field of military satellite communications, the requirement of secure communications security is even more crucial. How to realize the security of communications is a problem must be faced. A model for physical layer security communication in air-space-ground communication network was proposed which was a cooperative layer-direct connect mixed-to-ground physical layer secure communication model. Based on this model, the security of the system was further improved by studying the relay selection problem and the power distribution problem of satellite and relay, and an overall scheme to enhance the confidentiality of the communication network was also proposed.

**Key words:** air-space-ground communication network, physical layer security, relay selection, power allocation

收稿日期: 2018-01-08; 修回日期: 2018-03-12

基金项目: 国家自然科学基金资助项目 (No.61771169)

Foundation Item: The National Natural Science Foundation of China (No.61771169)



## 1 引言

### 1.1 研究的背景与意义

通信安全保密工作，关系到国家利益和军队的安全。为了谋求信息领域的领先地位，世界上许多国家将信息安全保密列为战略性课题，纷纷调整信息战略，大力开发信息攻防技术，建立健全信息安全保密组织和应急机制，促使传统的军事安全保密向现代化、技术化转变。“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兴产业，物理层安全，作为保证通信安全的一种新型手段，是该战略的一部分。

相比于有线通信，无线通信在广播性和传输信道的开放性方面具有优势，因此，无线通信在民用和军用方面得到了广泛应用。然而，广播及开放的特性也使得其缺乏物理边界约束，从而滋生无线安全问题。从物理层角度看，因为在无线覆盖范围内的任意通信节点均可以自由地收发信号，从而非法的恶意通信节点既可以被动地截获目标信号而不被发现，又可以主动地发送干扰信号以阻止正常通信。所以，无线通信将面临更严重的信息被窃取、身份位置信息泄露和恶意干扰等安全问题。

随着通信需求的不断扩展，由于陆地网络的局限性，空天地一体化网络成为大势所趋。然而空天地通信网络作为无线通信的典型应用，因其固有的广播性质和广泛的覆盖区域，面临严重的无线通信安全问题。尤其在军用卫星通信方面，安全通信保障要求更是至关重要的，如何实现通信的安全是一个必须要面对的问题。

传统的通信安全方式一般在网络层，例如参考文献[1-3]均是从网络层对安全进行分析，并且将大数据、云计算等新技术应用到网络安全的实现之中。然而，相比传统用于通信安全的密钥加密方式，新型并趋于实用的物理层安全技术作为一种新的选择，填补了密钥加密方式的许多不足，有着诸多优点。

- 物理层安全可以抵御量子攻击。一旦量子计算进入实用阶段，传统的加密方式在量子计算暴力分析下将受到极其严峻的挑战。
- 无线传播信道的唯一性、保密性、互异性提供了物理层安全的研究空间。多载波技术、多天线技术及协同中继技术等出现，增加了信号在频域和空域上的自由度。
- 无线传输技术与物理层安全技术有着天然的共性和联系，物理层安全实现方式更为便利。它不需要考虑其他的安全协议如何执行，也不需要消耗大量的通信资源或基础设施。并且，它还可以在解调之前快速验证节点的合法性，减少了浪费的信号处理，避免了非预期的传输。因此，物理层安全应该得到足够重视，可以预见，未来的安全通信必将结合物理层安全与传统安全。

卫星通信的广泛覆盖特性，在很多场景下成为军事通信的唯一途径，安全性必然成为其应用的痛点之一，因而备受关注。可以预见，物理层安全技术研究的发展，将为我国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 空天地通信网络面临的问题与挑战

目前关于卫星通信的物理层安全的研究有很多。参考文献[4]在2013年已经对卫星通信的物理层安全技术进行了研究展望。论述和分析了卫星通信物理层安全技术应用的可行性以及现有物理层安全技术应用于卫星通信的潜在问题，提出了卫星通信物理层安全可研究方向，展望了卫星通信物理层安全技术的发展前景。参考文献[5]在卫星通信网络中采用了动态波束成形技术，在卫星的边带处不能获取信息，从而实现了信息的安全性。参考文献[6]论述了使用物理层安全的多业务卫星通信，提出了一种新颖的设计，其针对固定、便携式、车载、船载和机载接收机中不同的速度和数据传输速率需求。对于固定接收机，本文提

出了一种利用物理层安全性的卫星通信资源优化方法,以适应不同数据传输速率的需求。参考文献[7]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(被动)窃听者包围。设计目标是通过发射波束形成最小化卫星上的总发射功率,同时满足个人预期用户的保密率限制。假设最先进的卫星信道模型,当窃听者的完美信道状态信息(CSI)可用于卫星时,提出了部分迫零方法来获得低复杂度的次优解。对于最优解,通过研究问题的凸性设计了一种结合半定规划松弛和基于梯度的方法的迭代算法。此外,探讨了使用人造噪声作为防止窃听者的额外自由度。当只有关于窃听者的部分CSI可用时,研究将窃听者的接收信号最小化为干扰加噪声比的问题。参考文献[8]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。讨论了基于窃听编码的卫星信道的无钥匙信息理论物理层安全的潜力。参考文献[9]研究了多波束卫星通信系统中的物理层安全性。首先,制定优化问题以最大化可实现的保密率的总和,同时满足机载卫星发射功率限制。然后,提出两种发射波束成形方案,即迫零和漏信噪比波束成形算法以获得BF加权向量以及功率分配系数。最后,仿真结果验证了两种方法的有效性,证明了漏信噪比波束成形算法优于迫零波束成形算法。参考文献[10]研究了多波束卫星网络中的物理层安全技术。物理层安全性是提高卫星通信系统的反拦截和反探测能力的有效途径。提出了波束成形和功率控制下多波束卫星网络物理层安全传输策略。研究了多波束卫星网络中下行链路评估的一组性能指标。参考文献[11]研究了发送者、合法接收者和窃听者均具有多天线的情况,并对两种情况进行了讨论。对于确定性场景,合法接收者和窃听者的信道矩阵固定且被所有节点知道;对于随机衰落场景,信道矩阵经历了块衰落,发送者仅有合法接收者

的CSI和窃听信道的统计CSI。在确定性场景中使用了GSVD方法,在高SNR下,获得保密容量,并且证明MISO情形下,任意SNR均可获得保密容量。另外,使用次优化的人工噪声时,它的性能在高SNR下的MISO情形下,能够获得保密容量。在衰落案例中,次优化的人工噪声使用依旧适用。对于独立瑞利衰落,如果窃听者的天线数大于或等于发送者天线数的2倍,同时增加发送者和窃听者的天线,保密容量接近零。参考文献[12]基于主信道和窃听信道均为莱斯衰落且相关位置信息被获得,当发送者和窃听者配备多根天线且不具有主信道和窃听信道的信道CSI时,获得了最佳的物理层安全性能。参考文献[13]在信道的CSI和波束成形权重固定的基础上,设计了在个体保密速率限制下的安全卫星系统,旨在最小化传输功率,提出了一个迭代算法来获得最优功率分配策略。然后,通过完全消除共信道干扰同时使窃听信号趋于零,获得次最优的波束成形权重。为了获得联合最优的功率分配和波束成形策略,评估了窃听CSI的影响。

根据已有的相关研究可知,预编码/波束成形技术的研究大都基于完美的合法信道和窃听信道的CSI,然而实际卫星通信场景中必然会有信道估计误差,所以在研究中需要考虑不完备CSI条件。同时,卫星天线数目受限也造成了目前的人工噪声技术的局限性。另外,卫星窃听者和合法用户在传统的模型下,无法解决信道几乎一致的问题,使得信道估计后的零空间,无法用于窃听者。

所以,空天地通信网物理层安全技术研究中需要解决以下问题。

#### (1) 物理层安全通信模型的构建与分析

需要建立与卫星通信中信道环境与参数相匹配的物理层安全模型,有针对性地研究星地通信系统物理层安全的基础理论与关键技术。

#### (2) 窃听者信道状态和位置

现有模型中,假定窃听者与合法接收者的信



道状态不同,具有不同的信道矩阵或向量。然而,很多情况下,星地链路的窃听者与合法接收者之间的距离,相对于星地的距离来说,可以认为很近,其信道状态可能与合法接收者的相同或相近,这种情况下,仅仅通过多波束成形等手段很难实现物理层上的安全传输。

(3) 非完备 CSI 信息的预编码和波束成形技术  
大部分文献对于发射信号设计进行了深入研究。在功耗等限制下,以实现最优或次最优发射信号设计为目标,同时重点考虑算法的计算复杂度。这对于整个卫星保密通信系统至关重要。然而,在设计发射信号时假设的场景中经常存在很多不合理的部分,如具有完备的窃听信道 CSI 等,这些假设能够使算法大大简化,从而得到精确或近似的闭合解或数值解。然而针对星地通信场景,由于反馈链路时延大,完备 CSI 信息的条件几乎无法满足,需要新的理论和算法来实现物理层安全通信。

#### (4) 人工噪声技术和天线数量

当使用通常的多波束成形和人工噪声来实现物理层安全时,为了能够使用 ZF 解耦多个用户,当窃听用户数量较多时,发射天线数量通常比较大,因此共信道波束间干扰和发射天线数量间的

矛盾还有待解决。

### 1.3 空天地通信网络安全通信的技术探索

空天地通信网络将位于地面、空中和太空的多种移动目标连接在一起,使得通信模型具有空间跨度大、时延长、信道反馈链路信息少的特性,但是卫星通信的覆盖面积广对物理层安全的关键技术的需求与地面通信完全不同。此外,由于时空约束及空间资源极度受限,空间信息通信的保密容量成为突出的瓶颈,其规划与优化利用往往不能采用传统的物理层安全理论和技术方法。所以,针对空天地通信网络实现物理层安全通信需要解决的问题,立足于协同中继、自组织网络技术、信道估计、部分 CSI 下的预编码和波束成形、人工噪声等物理层安全技术,对其进行技术创新,从而实现空天地通信网络的安全通信技术。具体的解决探索的方向如图 1 所示。

本文主要研究窃听者信道状态与位置这一空天地通信网络物理层安全需要解决的问题,建立了空天地通信网络的物理层安全通信模型——协作一直连混合星地物理层安全通信系统模型。在此模型的基础上,提出了需要研究的关键的技术优化问题,总结出了适应空天地通信网络的保密

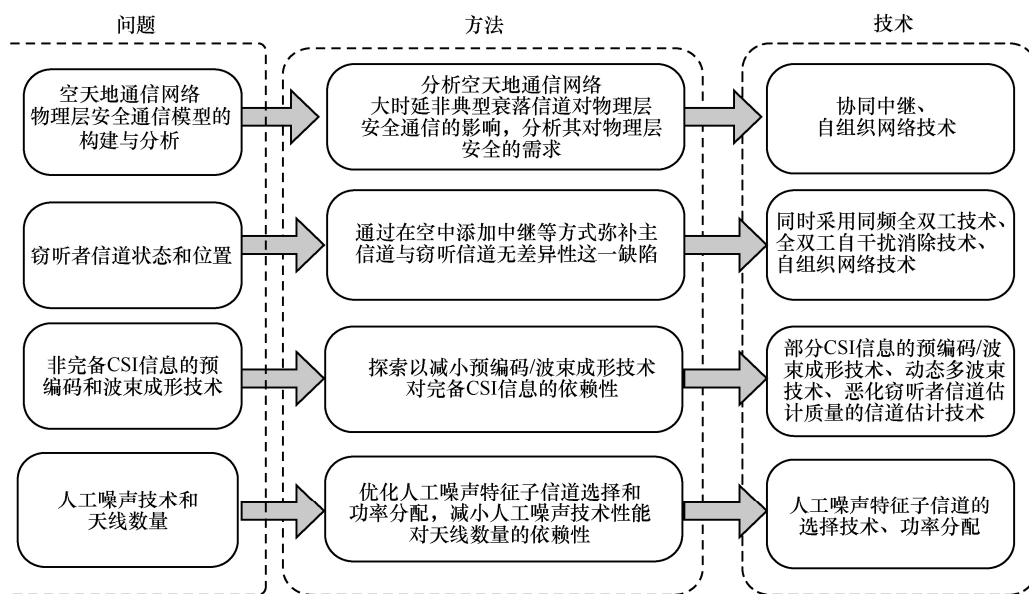


图 1 空天地通信网络物理层安全的探索方向

增强方案。

## 2 空天地通信网络的物理层安全通信模型的建立

### 2.1 基本的思想

在空天地通信网络中, 需要综合考虑窃听者距离合法接收者的相对位置。具体的可以分为如下两种情况。

- 窃听者与合法接收者间的距离很近, 相对于星地间的距离可以忽略不计, 此时主信道与窃听信道间近似相等。由于传统的地面无线通信的物理层安全技术均是利用主信道与窃听信道间的差异性, 所以不适用于该种情况。所以, 利用中继及同时同频全双工技术对卫星发送信息进行接收转发, 并按一定的策略发送干扰, 从而实现保密通信, 以弥补主信道和窃听信道相似这一弊端, 从而解决该情况下的物理层安全通信的问题。
- 窃听者与合法接收者距离足够远。该种情况下, 主信道与窃听信道的信道状态信息具有差异性, 与地面通信类似, 预编码、波束成形和人工噪声技术均可应用于该种情况下的星地安全通信。更直观的空天地通信网络安全通信的基本方案如图2所示。

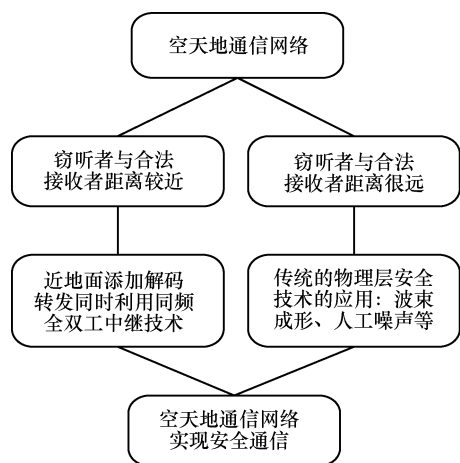


图2 空天地网络安全通信的基本方案

### 2.2 系统具体模型

由基本的思想, 提出协作一直连混合星地物理层安全通信系统模型。与传统卫星通信中的中继卫星不同, 通常的卫星通信由高轨卫星进行信息中继。本模型中的中继, 可以充分利用卫星、飞机、热气球等现有的浮空平台资源作为同时同频全双工中继, 具有实际的应用意义, 便于实际的工程实现。

假设空天地通信网络中, 星地间链路的信道建模为弱莱斯信道, 多天线合法发射者 Alice (代表卫星) 的目标是向合法接收者 Bob1 和 Bob2 分别发送数据信息。系统中有  $M$  个同时同频全双工的 Relay (中继), Eve1 和 Eve2 分别想要窃听 Bob1 和 Bob2 的消息。Bob1 和 Eve1 间的距离很近, 在  $M$  个 Relay 中选择与 Alice 和 Bob1 近似共线的 Relay  $k$  作为数据消息传输的 DF (decode forward) 中继 (卫星、飞机、热气球等)。Alice 将数据信息发送给 Relay  $k$ , Relay  $k$  接收 Alice 想要发送给 Bob1 的信号并进行解码, 与此同时向 Bob1 发送前一时隙的解码的信号。假设 Bob1 只能接收到 Relay  $k$  的信号。Eve 可同时接收到来自 Alice 和 Relay  $k$  的信号。Bob2 和 Eve2 距离很远, Alice 不通过中继, 直接向 Bob2 发送数据信息, Eve2 接收 Alice 的信号对 Bob2 进行窃听。Alice、Bob、Relay 和 Eve 分别装有  $N_s$ 、 $N_d$ 、 $N_r$  和  $N_e$  根天线。Alice 到 Bob、Eve 和 Relay 的信道矩阵分别为  $H_{sd}$ 、 $H_{se}$  和  $H_{sr}$ , Relay 到 Bob 和 Eve 的信道矩阵为  $H_{rd}$  和  $H_{re}$ , 图3给出了具体的系统模型示意。

由此图3中模型可知, 窃听者 Eve 距离合法接收者 Bob 的远近决定了系统的数据传输模式。所以系统的保密容量与窃听者与合法接收者 Bob 的远近有关, 因此, 分为以下两种情况讨论系统的保密容量。

(1) 协作模型: 窃听者 Eve 在其合法接收者 Bob 的附近

图3 模型中的 Bob1 和 Eve1 就是这种情况。

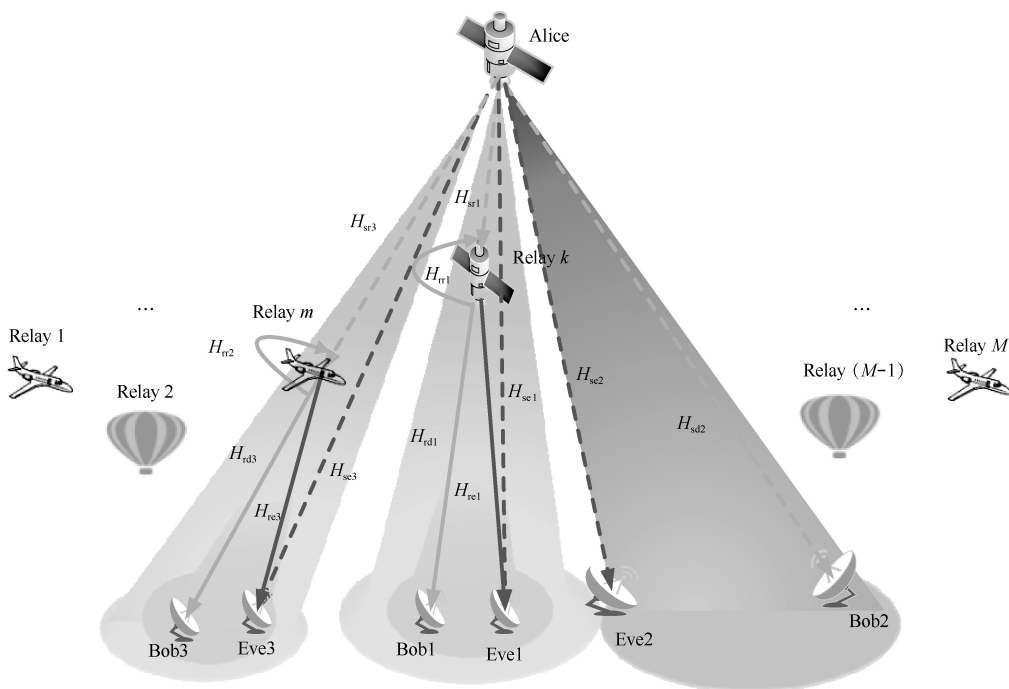


图3 空天地通信网物理层安全系统模型示意

Alice 发送有用的数据信号给中继 Relay  $k$ , Relay  $k$  接收并解码信号, 同时向 Bob1 发送上一时刻的数据信号, Bob1 仅能接收到 Relay  $k$  的信号, Eve 可接收到 Alice 和 Relay  $k$  的信号, 也就是上一时刻数据信号和此时此刻数据信号的叠加, 使接收到的信号质量下降, 从而获得保密容量。至于具体的 Alice 和 Relay  $k$  的发射功率的设定及中继的选择问题, 需要进行数学上的优化, 从而实现最优的保密容量。

(2) 直连模型: 合法接收者 Bob 距离窃听者较远

图3模型中的 Bob2 和 Eve2 就是这种情况。Alice 发射通过波束成形, 发射有用的数据信号和人工噪声, 从而提高 Bob 端的信号质量, 降低 Eve2 端的信号质量, 获得保密容量。同时, 需要优化设计最优的波束成形矩阵及人工噪声, 使保密容量最大化, 系统的保密性能最优化。

### 3 空天地通信网络物理层安全的关键技术与保密性增强方案

如图3所示, 空天地通信网物理层安全系统

模型分为两种: 协作模型中 Alice 和 Relay  $k$  间的发射功率的分配及中继的选择问题以及直连模型中波束成形矩阵和人工噪声的设计及人工噪声的功率大小问题, 两者对系统的保密性能均会产生影响。所以, 对上述影响保密性能的因素进行合理的优化, 可以增强系统的保密性能。

#### 3.1 协作模型的中继选择优化

不同的中继节点与 Alice、Bob 和 Eve 间的信道状态不同, 所以同一 Bob 和 Eve 的情况下, 选择不同的中继进行解码转发所达到的保密性能会有很大的差异性。为了获得最佳的保密性, 需要在所有覆盖的  $M$  个中继中选择最优的中继进行数据转发传输。

假设 Alice 发送有用的数据信号给中继 Relay  $k$  ( $k=1,2,\dots,M$ ), Relay  $k$  接收并解码信号, 同时向 Bob1 发送上一时刻的数据信号, Bob1 仅能接收到 Relay  $k$  的信号, Eve 可接收到 Alice 和 Relay  $k$  的信号。那么在 Bob1 端和 Eve1 端接收到的信号分别为:

$$y_{d1} = H_{rd,k}^H x' + n_{d1,k}, \quad k=1,2,\dots,M \quad (1)$$

$$y_{el} = H_{sel,k}^H x + H_{rel,k}^H x' + n_{el,k}, \quad k=1,2,\dots,M \quad (2)$$

其中,  $H_{rd1,k}$  是 Bob1 和 Relay  $k$  间的信道状态矩阵,  $H_{rd1,k} \in C^{N_r \times N_d}$ ,  $H_{rel,k}$  是 Eve1 和 Relay  $k$  间的信道状态矩阵,  $H_{rel,k} \in C^{N_r \times N_e}$ ,  $H_{sel,k}$  是 Alice 和 Eve1 间的信道状态矩阵,  $H_{sel,k} \in C^{N_s \times N_e}$ ,  $x$  是 Alice 发射出的信号,  $x \in C^{N_s}$ ,  $x'$  是 Relay 发射出的信号,  $x' \in C^{N_r}$ ,  $n_{d1,k}$  是在 Bob1 接收端的噪声,  $n_{d1,k} \in C^{N_d}$ ,  $n_{d1,k} \sim \text{CN}(0, \sigma_{d1}^2)$ ,  $n_{el,k}$  是在 Eve1 接收端的噪声,  $n_{el,k} \in C^{N_e}$ ,  $n_{el,k} \sim \text{CN}(0, \sigma_{el}^2)$ 。

那么 Bob1 和 Eve1 接收到的有用信号的信干噪比为:

$$\text{SINR}_{d1} = \frac{x'^H H_{rd1,k} H_{rd1,k}^H x'}{\sigma_{d1,k}^2} \quad (3)$$

$$\text{SINR}_{el} = \frac{x'^H H_{rel,k} H_{rel,k}^H x'}{x^H H_{sel,k} H_{sel,k}^H x + \sigma_{el,k}^2} \quad (4)$$

则直连模型的保密容量为:

$$C_{s1} = \frac{1}{2} \text{lb}(1 + \text{SINR}_{d1,k}) - \frac{1}{2} \text{lb}(1 + \text{SINR}_{el,k}) \quad (5)$$

所以, 最优的中继  $k$  可以通过式 (6) 确定:

$$k = \arg \max_{k=1,2,\dots,M} \left[ \frac{1}{2} \text{lb}\left(1 + \frac{x'^H H_{rd1,k} H_{rd1,k}^H x'}{\sigma_{d1,k}^2}\right) - \frac{1}{2} \text{lb}\left(1 + \frac{x'^H H_{rel,k} H_{rel,k}^H x'}{x^H H_{sel,k} H_{sel,k}^H x + \sigma_{el,k}^2}\right) \right] \quad (6)$$

### 3.2 协作模型的功率分配优化

在同时同频全双工中继已经确定的基础上, Alice 和 Relay 总的发射功率一定, Alice 与 Relay 各占的发射功率大小会对系统的保密容量产生影响, 而 Alice 和 Relay 间发射功率的合理分配, 能够使系统的保密性能得到进一步的提升。

假定 Alice 和 Relay  $k$  ( $k$  为  $1, \dots, M$  中一确定值) 的总发射功率约束为  $P$ , Alice 的发射功率约束为  $\alpha P$ , Relay  $k$  的发射功率为  $(1-\alpha)P$ , 其中,  $\alpha$  为功率分配因子,  $0 < \alpha < 1$ 。Alice 发送有用的数据信号给中继 Relay  $k$ , Relay  $k$  接收并解码信号, 同时向 Bob1 发送上一时刻的数据信号, Bob1

仅能接收到 Relay  $k$  的信号, Eve 可接收到 Alice 和 Relay  $k$  的信号。那么, 在 Bob1 端和 Eve1 端接收到的信号分别为:

$$y_{d1} = \sqrt{(1-\alpha)P} H_{rd1,k}^H x' + n_{d1} \quad (7)$$

$$y_{el} = \sqrt{\alpha P} H_{sel,k}^H x + \sqrt{(1-\alpha)P} H_{rel,k}^H x' + n_{el,k} \quad (8)$$

其中,  $H_{rd1,k}$  是 Bob1 和 Relay  $k$  间的信道状态矩阵,  $H_{rd1,k} \in C^{N_r \times N_d}$ ,  $H_{rel,k}$  是 Eve1 和 Relay  $k$  间的信道状态矩阵,  $H_{rel,k} \in C^{N_r \times N_e}$ ,  $H_{sel,k}$  是 Alice 和 Eve1 间的信道状态矩阵,  $H_{sel,k} \in C^{N_s \times N_e}$ ,  $x$  是 Alice 发射出的信号,  $x \in C^{N_s}$ ,  $x'$  是 Relay 发射出的信号,  $x' \in C^{N_r}$ ,  $n_{d1,k}$  是在 Bob1 接收端的噪声,  $n_{d1,k} \in C^{N_d}$ ,  $n_{d1,k} \sim \text{CN}(0, \sigma_{d1}^2)$ ,  $n_{el,k}$  是在 Eve1 接收端的噪声,  $n_{el,k} \in C^{N_e}$ ,  $n_{el,k} \sim \text{CN}(0, \sigma_{el}^2)$ 。

那么 Bob1 和 Eve1 接收到的有用信号的信干噪比为:

$$\text{SINR}_{d1} = \frac{(1-\alpha)P x'^H H_{rd1,k} H_{rd1,k}^H x'}{\sigma_{d1,k}^2} \quad (9)$$

$$\text{SINR}_{el} = \frac{(1-\alpha)P x'^H H_{rel,k} H_{rel,k}^H x'}{\alpha P x^H H_{sel,k} H_{sel,k}^H x + \sigma_{el,k}^2} \quad (10)$$

则直连模型的保密容量为:

$$C_1 = \frac{1}{2} \text{lb}(1 + \text{SINR}_{d1,k}) - \frac{1}{2} \text{lb}(1 + \text{SINR}_{el,k}) \quad (11)$$

所以, 最优的功率分配因子  $\alpha$  可以通过式 (12) 求得:

$$\alpha = \arg \max_{0 < \alpha < 1} \left[ \frac{1}{2} \text{lb}\left(1 + \frac{(1-\alpha)P x'^H H_{rd1,k} H_{rd1,k}^H x'}{\sigma_{d1,k}^2}\right) - \frac{1}{2} \text{lb}\left(1 + \frac{(1-\alpha)P x'^H H_{rel,k} H_{rel,k}^H x'}{\alpha P x^H H_{sel,k} H_{sel,k}^H x + \sigma_{el,k}^2}\right) \right] \quad (12)$$

### 3.3 直连模型中波束成形与人工噪声的联合设计

通过设计波束成形矩阵, 可以使合法接收者接收到的有用信号强度尽可能地提升, 窃听者接收到的有用信号强度尽可能地降低, 从而获得保密性能的提升。通过设计人工噪声, 可以使其对合法接收者的干扰尽可能地小, 对窃听者的干扰尽可能地大, 从而提升保密性。由于波束成形和人工噪声的



设计均与主信道和窃听信道等参数息息相关,所以需要在一起进行考虑,联合进行优化设计。

Alice 发射通过波束成形,发射有用的数据信号和人工噪声,则 Bob2 和 Eve2 可接收到的信号分别为:

$$y_{d2} = H_{sd2}^H Ws + H_{sd2}^H a + n_{d2} \quad (13)$$

$$y_{e2} = H_{se2}^H Ws + H_{se2}^H a + n_{e2} \quad (14)$$

其中,  $s$  是 Alice 想要发送给 Bob2 的有用数据信号矢量,  $s \in C^p$ ,  $W$  是 Alice 到 Bob2 的波束成形矩阵,  $W \in C^{N_s \times p}$ ,  $H_{sd2}$  为 Alice 与 Bob2 间的信道状态矩阵,  $H_{sd2} \in C^{N_s \times N_d}$ ,  $H_{se2}$  为 Alice 与 Bob2 间的信道状态矩阵,  $H_{se2} \in C^{N_s \times N_e}$ ,  $a$  是 Alice 发射的人工噪声,  $a \in C^{N_s}$ ,  $n_{d2}$  是在 Bob2 接收端的噪声,  $n_{d2} \in C^{N_d}$ ,  $n_{d2} \sim \text{CN}(0, \sigma_{d2}^2)$ ,  $n_{e2}$  是在 Eve2 接收端的噪声,  $n_{e2} \in C^{N_e}$ ,  $n_{e2} \sim \text{CN}(0, \sigma_{e2}^2)$ 。

那么 Bob2 和 Eve2 接收到的有用信号的信干噪比为:

$$\text{SINR}_{d2} = \frac{s^H W^H H_{sd2} H_{sd2}^H Ws}{a^H H_{sd2} H_{sd2}^H a + \sigma_{d2}^2} \quad (15)$$

$$\text{SINR}_{e2} = \frac{s^H W^H H_{se2} H_{se2}^H Ws}{a^H H_{se2} H_{se2}^H a + \sigma_{e2}^2} \quad (16)$$

则 Bob2 处在该情况下的保密容量上界为:

$$C_{s2} = \frac{1}{2} \log \left( 1 + \frac{s^H W^H H_{sd2} H_{sd2}^H Ws}{a^H H_{sd2} H_{sd2}^H a + \sigma_{d2}^2} \right) - \frac{1}{2} \log \left( 1 + \frac{s^H W^H H_{se2} H_{se2}^H Ws}{a^H H_{se2} H_{se2}^H a + \sigma_{e2}^2} \right) \quad (17)$$

最优的波束成形矩阵和人工噪声矩阵可以通过下面的优化问题确定。

$$\begin{aligned} (W, a) = \arg \max & \frac{1}{2} \log \left( 1 + \frac{s^H W^H H_{sd2} H_{sd2}^H Ws}{a^H H_{sd2} H_{sd2}^H a + \sigma_{d2}^2} \right) - \\ & \frac{1}{2} \log \left( 1 + \frac{s^H W^H H_{se2} H_{se2}^H Ws}{a^H H_{se2} H_{se2}^H a + \sigma_{e2}^2} \right) \\ \text{s.t. } & \text{tr}(W^H W) \leq 1; \\ & \text{tr}(a^H a) \leq 1; \end{aligned} \quad (18)$$

### 3.4 空天地通信网络物理层安全的保密容量增强方案

根据合法接收者与窃听者间的距离的不同情况,确定在空天地通信网络物理层安全通信模型中的具体情况,进行进一步的保密容量优化增强。针对空天地通信网络物理层安全通信模型中的协作模型,可以先假设 Alice 和合法接收者间的功率是均匀分配的,然后进行同时同频全双工中继选择的优化,从而确定进行传输的中继节点。继而进行进一步的 Alice 与已选择的中继节点间的功率分配方案。针对其中的直连模型,进行波束成形矩阵和人工噪声的联合优化设计,如图 4 所示。

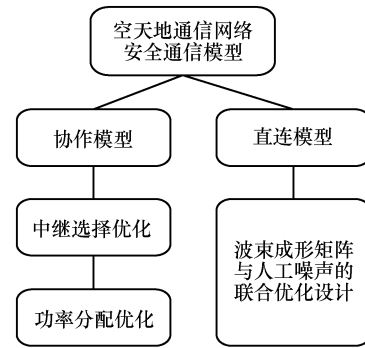


图 4 空天地通信网络的保密容量增强方案

因此,协作一直连混合星地物理层安全通信系统模型可以实现空天地通信网络的安全通信,同时通过上述的保密容量增强方案进一步提升系统的保密性能。最终,实现空天地通信网络较好的安全通信。

## 4 结束语

本文提出了空天地通信网络的物理层安全通信模型——协作一直连混合星地物理层安全通信系统模型。利用同时同频全双工协作中继解决了当地面的窃听者与合法用户间距离很近时,信道近似相等从而传统的地面物理层安全技术不适用的问题。同时进一步研究了基于空天地通信网络的物理层安全通信模型的保密容量的增强的方案,具体研究了协作模型中 DF 中继的中继

选择和 DF 中继与卫星间的功率分配比的优化, 直连模型中卫星的波束成形矩阵和人工噪声的优化, 最后提出了适应空天地通信网络的保密增强方案, 尽可能地提高了空天地通信网络的安全性。

## 参考文献:

- [1] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.  
WU J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014, 30(7): 2-7.
- [2] 刘明辉, 张尼, 张云勇, 等. 云环境下的敏感数据保护技术研究[J]. 电信科学, 2014, 30(11): 2-8.  
LIU M H, ZHANG N, ZHANG Y Y, et al. Research on sensitive data protection technology on cloud computing [J]. Telecommunications Science, 2014, 30(11): 2-8.
- [3] 王帅, 汪来富, 金华敏, 等. 网络安全分析中的大数据技术应用[J]. 电信科学, 2015, 31(7): 145-150.  
WANG S, WANG L F, JIN H M, et al. Big data application in network security analysis [J]. Telecommunications Science, 2015, 31(7): 145-150.
- [4] 张应宪, 刘爱军, 王永刚. 卫星通信物理层安全技术研究展望[J]. 电讯技术, 2013, 53(3): 363-370.  
ZHANG Y X, LIU A J, WANG Y G. Prospect of physical layer security technology research in satellite communication[J]. Telecommunication Engineering, 2013, 53(3): 363-370.
- [5] GAO Y, AO H, FENG Z, et al. Modeling and practise of satellite communication systems using physical layer security: a survey[C]//IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), July 22-23, 2017, Guangzhou, China. Piscataway: IEEE Press, 2017: 829-832.
- [6] YUAN GAO, HONG AO, QUAN ZHOU, et al. Modeling of satellite communication systems design with physical layer security[C]//International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), March 23-25, 2016, Chennai, India. [S.l.:s.n.], 2017: 1680-1683.
- [7] 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.
- [8] ÁNGELES VAZQUEZ-CASTRO, HAYASHI M. Information-theoretic physical layer security for satellite channels[C]// Aerospace Conference, March 4-11, 2017, Big Sky, MT, USA. Piscataway: IEEE Press, 2017: 1-14.
- [9] LU W X, JIANG Y W, YIN C Y, et al. Security beamforming algorithms in multibeam satellite systems[C]//IEEE 2nd Advanced Information Technology, Electronic and Automation

Control Conference (IAEAC), March 26-27, 2017, Chongqing, China. [S.l.:s.n.], 2017: 1272-1277.

- [10] MA D, LIU X, WANG X, et al. On the performance indexes of physical layer security for multi-beam satellite networks[C]// International Conference on Wireless Communications & Signal Processing, October 15-17, 2015, Nanjing, China. Piscataway: IEEE Press, 2015: 1-6.
- [11] KHISTI A, WORNELL G, WIESEL A, et al. On the Gaussian MIMO wiretap channel[C]//IEEE International Symposium on Information Theory, June 24-29, 2007, Nice, France. Piscataway: IEEE Press, 2007: 2471-2475.
- [12] YAN S, MALANEY R. Location-based beamforming for enhancing secrecy in Rician wiretap channels[J]. IEEE Transactions on Wireless Communications, 2016, 15(4): 2780-2791.
- [13] VAZQUEZ-CASTRO M A, HJORUNGNES A. Secure satellite communication systems design with individual secrecy rate constraints[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3): 661-671.

## 作者简介



韩帅 (1981-), 男, 博士, 哈尔滨工业大学副教授、博士生导师, 主要研究方向为卫星通信、宽带无线通信、无线通信与导航对抗、室内定位。



台祥雪 (1993-), 女, 哈尔滨工业大学硕士生, 主要研究方向为卫星通信与物理层安全。



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、长聘教授、博士生导师。主持完成科研工作 30 余项, 包括 3 项国家“863”计划、5 项国家自然科学基金和 4 项国家重大科技专项, 获得省部级科技成果奖 10 项, 授权国家发明专利 60 余项。2005 年获得优秀黑龙江省留学人员报国奖,

2008 年入选教育部新世纪优秀人才支持计划, 2014 年当选哈尔滨市优秀学科带头人。兼任中国电子学会会士、黑龙江省电子学会常务理事、中国电子学会信号处理分会委员、IEEE 通信学会哈尔滨分会主席、《IEEE Communication Magazine》等多个国际权威杂志的编委。