

天地一体化信息网络中物理层安全方案

马方舒, 王 岩, 张国威, 程宇新
(北京大学信息与通信研究所, 北京 100871)

摘要: 首先阐述当前主流的物理层安全技术, 并介绍相关技术指标; 然后针对天地一体化信息网络中的3种典型场景, 对其中物理层安全方面的相关研究进行阐述; 最后, 针对3种典型场景的物理层安全提出需要解决的问题, 并对可行性方案进行探讨。

关键词: 天地一体化信息网络; 物理层安全; 网络架构; 卫星通信

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.2096-8930.20200210

Physical Layer Security Schemes in Space-Integrated-Ground Information Network

MA Fangshu, WANG Yan, ZHANG Guowei, CHENG Yuxin
Institute of Information and Communication Technology, Peking University, Beijing 100871, China

Abstract: Firstly, the current mainstream technologies of physical layer security were summarized and the relevant technical indicators were introduced; Then, the research on physical layer security in three typical scenarios of the space-integrated-ground information network was summarized; Finally, problems need to be solved for the physical layer security of the three typical scenarios were proposed, and feasible schemes were discussed.

Keywords: space-integrated-ground information network, physical layer security, network architecture, satellite communication

1 引言

天地一体化信息网络是在国家战略需求的引领下, 在地面网络基础上融合空间网络, 实现天、空、地三网协同, 并为全球范围内陆、海、空、天各类用户提供可随时接入的安全保质的公用信息基础设施^[1]。

从太空到地面, 天地一体化信息网络架构可分为3个不同的部分, 如图1所示。第一部分是天基骨干网, 一般由通信、导航、遥感卫星, 以及其他靠近地球同步轨道的天基骨干节点组成。其中, 地球同步轨道 (Geostationary Earth Orbit, GEO) 卫星具备计算和存储能力, 可以直接与地面设备通信, 但由于往返时间较长, 时延成为主要的约束条件。而中轨 (Medium Earth Orbit, MEO) 卫星具有移动性, 属于非同步卫星, 主要用于导航和地面移动通信系统的补充。天基骨干网主要负责骨干网互联、骨干网接入和网络管理。

第二部分是天基接入网, 由宽带卫星接入网、移动卫星接入网、低轨 (Low Earth Orbit, LEO) 卫星接入网和近地接入网组成。其中, LEO卫星在同地面通信时具有更短时延, 特别是从地面站到LEO卫星的时延可以减少到 $1 \sim 4 \text{ ms}$ ^[2]。近地接入网包括各类飞行器, 如飞机、飞艇、热气球以及无人机等。天基接入网主要负责实现具有星间链路的空间物联网, 以及天基骨干网和地基骨干网之间的数据交换和中继任务。

第三部分是由移动接入网、固定移动接入网、移动网络和基站组成的地基网络, 主要负责实现地面网络间的互联互通。地基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回的数据。因此, 发展成熟的地基网络主要为人口密集地区提供高速服务。而卫星网络可在高峰期作为辅助, 分担地面网络的流量, 二者相辅相成。

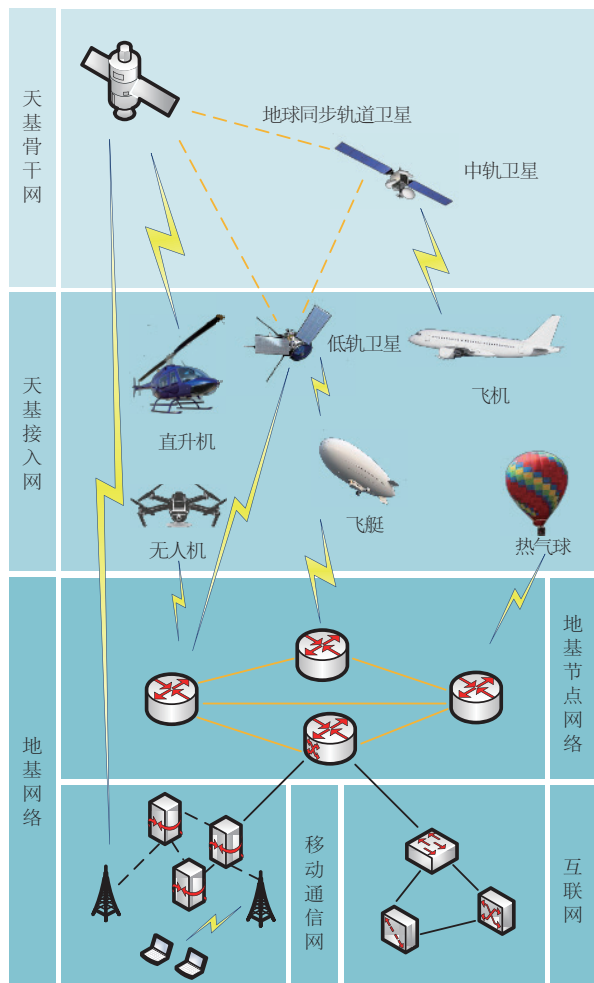


图1 天地一体化信息网络典型架构

2 物理层安全技术

天地一体化信息网络充分利用天、空、地的网络资源，使得各层通信设施开放互联，让用户随时随地享受到便利的无线连接。作为天地一体化信息网络的重要组成部分，卫星通信系统覆盖范围广、广播和组播能力强，尤其可为偏远地区或紧急通信提供服务，近年来愈发受到重用。但卫星通信系统的高覆盖范围和广播特性为窃听者提供了天然的窃听条件，使得信息传输会暴露在被动窃听和主动干扰之下。所以无线通信可能会受到窃听、流量分析、消息修改、伪装攻击、拒绝服务等诸多物理层攻击^[3]。正如安全领域所提到的，一个系统的稳健性往往取决于其最薄弱的环节。因此，如何有效提升天地一体化信息网络在物理层的安全性成为亟待解决的问题。

传统的提升物理层安全技术属于计算安全类，包括公钥加密和对称密钥加密。传统的加密方法在大多数情

况下是有效的，但其固有的弱点是计算量大和密钥管理成本高，可能导致高复杂性和高资源消耗；而且，不能随着信道的变化而灵活地适应，无法保证非法窃听者使用暴力算法时不能被破解。于是，利用无线信道的唯一性、时间可变性及空间去相关性等特质增强物理层安全的方法受到众多学者的关注。与传统的密钥加密方法相比，基于信息论的PLS（Physical Layer Security，物理层安全）方法优点有：物理层安全可从信息论角度证明有实现完全保密的能力，不可通过蛮力计算破解^[4]；具有轻量级的计算复杂性和资源需求，可适用于大规模通信加密的5G时代；具有良好的适应物理层变化的能力，可通过优化系统参数和传输方案来适应无线信道的变化。基于信息论安全的PLS方法可分为物理层编码、资源分配、信号处理、多点协作、密钥生成和物理层授权等。总的来说，常见的增强物理层安全的方法及分类如图2所示。

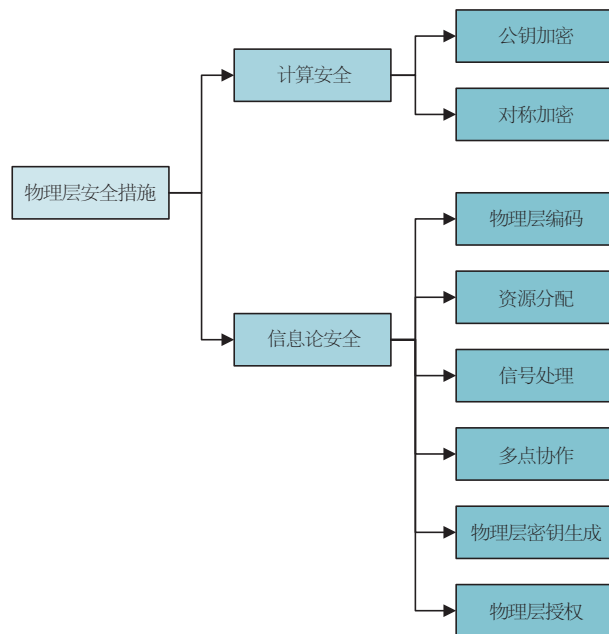


图2 常见的增强物理层安全的方法及分类

WYNER^[5]在1975年提出窃听信道模型，在不需要密钥的情况下利用合法信道和非法信道之间的差异，可在物理层上实现完全保密。因为在窃听信道模型中，窃听者接收到的信号是合法用户接收信号衰减的结果。WYNER还证明了离散无记忆信道的保密容量为合法链路的互信息与窃听链路的互信息之差的最大值。在此基础上，之后的众多学者主要将对基于信息论的PLS技术研究集中在两个部分：一是从信息论的角度提升保密容量等保密系统评价指标；二是从优化和信号处理的角度设计信息传输安全系统^[6]。

用来评价通信系统保密能力的常见指标有保密容量 (Secrecy Capacity, SC)、保密中断概率 (Secrecy Outage Probability, SOP)、安全能量效率 (Secrecy Energy Efficiency, SEE) 等。

(1) 保密容量, 被定义为主信道和窃听信道的信道容量之差, 即 $C_S = \max(C_B - C_E, 0)$, 其中 $C_B = \log_2(1 + \gamma_B)$ 是合法信道的信道容量, $C_E = \log_2(1 + \gamma_E)$ 是窃听信道的信道容量, γ_B 和 γ_E 分别代表合法接收者和窃听者的信噪比。

(2) 保密中断概率, 是用来衡量无线通信系统服务质量的重要指标, 被定义为瞬时的信道容量小于可接受的容量阈值 C_0 的概率, 公式为 $P_{\text{out}}(C_0) = \Pr(C_S < C_0) = \Pr(\gamma_B < \gamma_0 + \gamma_E(1 + \gamma_0))$ 。

(3) 安全能量效率, 在能量资源有限的情况下评估系统保密性能的指标, 定义为每单位能量消耗的安全容量, 即 $\eta = (R_S/E) [\text{bit/J}]$, E 为系统的能量消耗。

再看天地一体化信息网络, 卫星通信网络的高覆盖范围使得合法通信链路更加容易受到物理层攻击, 且天、空、地不同层级的通信设施间可能存在不同的信道条件, 所需要耗费的计算资源更加巨大。故在天地一体化信息网络中, 需要引入基于信息论的PLS技术, 在相对有限的计算资源下利用信道本身的特点保证系统通信时的物理层安全。

3 典型物理层安全架构

由于天地一体化信息网络涉及天、空、地3个维度多个通信设施, 每个通信设施所扮演的角色也各有不同, 故将众多学者所提出的经典信息网络架构组成元素及角色分类汇总, 具体见表1。

表1 经典信息网络架构组成元素及角色分类汇总

维度	通信设施	角色
天	LEO、MEO、GEO卫星	发送者/接收者
空	无人机、飞艇、热气球、飞机等	发送者/接收者、中继/干扰、合法用户/窃听者
地	基站、移动用户、路由器等	发送者/接收者、中继/干扰、合法用户/窃听者

根据卫星所覆盖的地面范围以及是否需要通过中继传送信息给合法用户, 可将天地一体化信息网络分为3类: 陆地移动卫星网络 (Land Mobile Satellite Networks, LMSN)、异构星地中继网络 (Hybrid Satellite-Terrestrial Relay Networks, HSTRN)、星地集成网络 (Satellite-Terrestrial Integrated Networks, STIN)。本节将对已有的3种典型网络架构进行梳理, 并把物理层安全相关的研究进行汇总。

3.1 陆地移动卫星网络

LMSN是新兴的航空航天和信息技术网络, 可为陆地移动用户提供高吞吐量和无缝连接服务, 特别是在地面通信无法建立的偏远地区。LMSN的物理层安全需要部署便捷、波束或能量方向灵活可变的节点, 而无人机 (Unmanned Aerial Vehicle, UAV) 具有低成本、高速、无线覆盖和可移动性等优点, 因而许多学者提出了结合UAV的LMSN物理层安全传输方案。将UAV引入LMSN后可用于广播、监视、救援和导航等场景, 但是, 这种机载通信基础设施更容易受到窃听和安全威胁。在LMSN中, UAV可以作为友好干扰器广播噪声, 减少窃听信道的保密容量, 从而增大合法信道与窃听信道的保密容量之差, 典型架构如图3所示。参考文献[7]在卫星向地面用户发送信息的同时引入产生友好干扰的UAV, 并推导出LMSN在卫星链路和UAV的异构信道下的SOP。仿真结果表明, 虽然卫星信道条件对LMSN系统性能有严重影响, 但UAV干扰机可以显著提高保密性能。参考文献[8]在图3模型的基础上, 假设合法用户和窃听者物理距离很近, 具有相似的卫星通信信道。于是引入多个飞机和气球作为近地共频同时干扰中继, 发送理论上对合法用户无影响的干扰信号; 并推导了已知瞬时CSI (Channel State Information, 信道状态信息) 和统计CSI条件下的中继选择标准, 从而最大限度地降低了SOP。

此外, 在没有UAV发送干扰信号的场景下, 由一颗卫星、一个合法用户和一个或多个窃听者组成的架构也被众多学者所研究, 如图4所示。参考文献[9]得到了多个窃听者在阴影-莱斯衰落信道下系统精确和渐近的SOP表达式, 并提出两个关键的性能指标, 即保密分集阶数和保密阵列增益。分析仿真结果可知, 保密分集的阶数只与合法接收者的天线数目有关, 而与信道估计信息的不完善以及主信道和窃听者信道的遮蔽严重程度无关。

3.2 异构星地中继网络

由于LMSN中卫星用户和地面用户之间的链路可能受限于障碍物或阴影造成的掩蔽效应^[10], 故无法实现直接传输, 尤其是当卫星仰角较低或地面用户为室内用户时。为了克服这一问题, 具有广泛覆盖区域、能实现高传输速率的HSTRN应运而生。这样一来, 卫星网络可以充分利用成熟的地面中继站, 卫星信号可以在地面中继站的协助下可靠地转发给地面用户。

一般的HSTRN架构主要由卫星、地面基站、合法用户及一个或多个窃听者组成。由于雨雪等天气的影响, 卫星和合法用户之间没有直接可靠的传输链路。两阶段多窃听者的HSTRN架构^[11]如图5所示, 窃听用户可能在

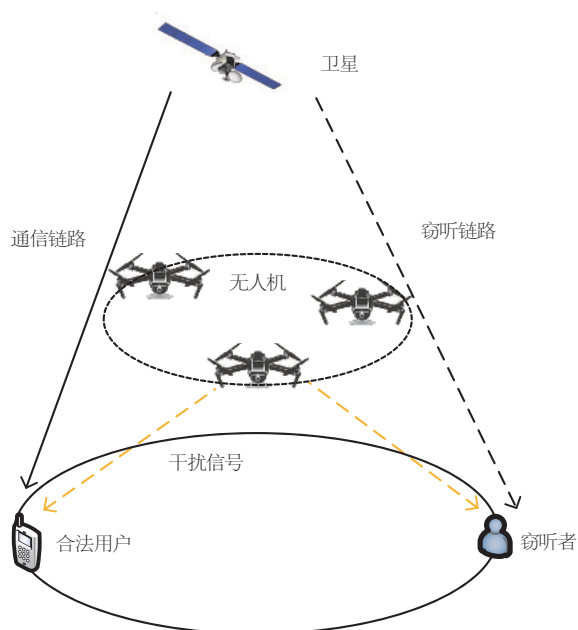


图3 无人机发送友好干扰信号的LMSN典型架构

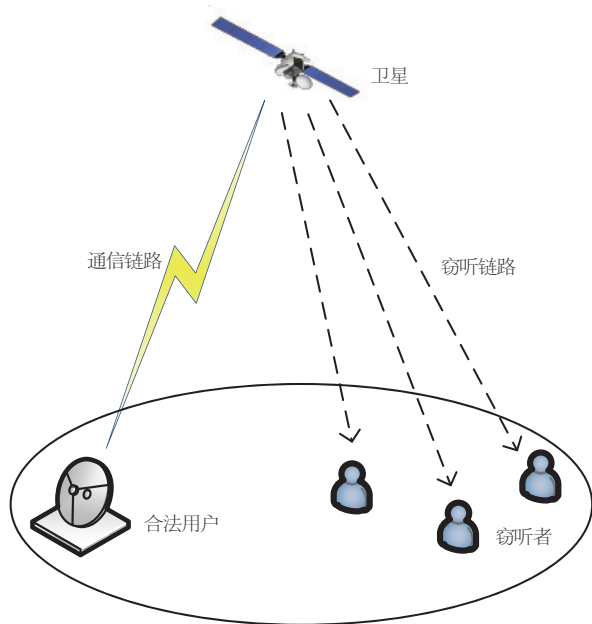


图4 多个窃听者存在的LMSN架构

卫星-中继链路窃听，也可能在中继-合法用户链路窃听，且可有多个窃听者存在。参考文献[11]就此模型提出两种针对PLS的方案：方案一为在卫星-中继和中继-合法用户之间选择更大的保密容量；方案二为在卫星-中继和中继-合法用户之间选择较小的保密容量。另外，推导出了两种方案下的保密中断概率的封闭表达式，为选择方案和评估系统参数对保密系统性能的影响提供了一种快速的分析方法。研究表明，随着窃听者数量的增

加，窃听功率增大和信道衰落会导致系统的SOP降低。同时证明了采取方案一可以得到系统的最佳保密性能，而采用方案二只能得到保密性能最差的系统。

此外，因为UAV具有尺寸小、可移动及低成本等优点，可被部署为5G通信的空中无线接入平台（如基站、移动中继、回程等）；而将UAV融入HSTRN并探讨PLS技术已成为近来的研究热点。参考文献[12]提出了一种新型的基于编码转发、由UAV做中继的HSTRN的三维架构。其中，窃听者也是UAV，可围绕UAV中继平面飞行，系统架构如图6所示，并推导出最近无人机中继选择（Closest UAV Relay Selection, CURS）和均衡无人机中继选择（Uniform UAV Relay Selection, UURS）两种策略的精确非零保密容量概率（Probability of Non-Zero Secrecy Capacity, PNZSC）和SOP的表达式及上下界。

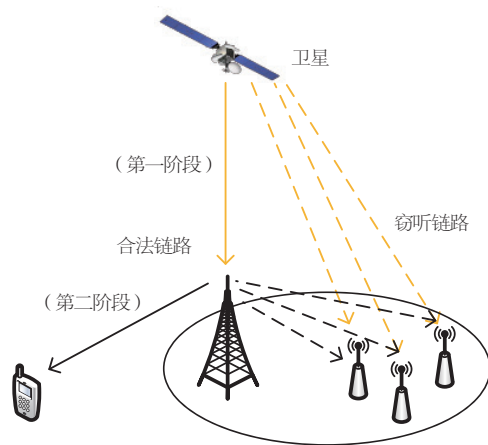


图5 两阶段多窃听者的HSTRN架构

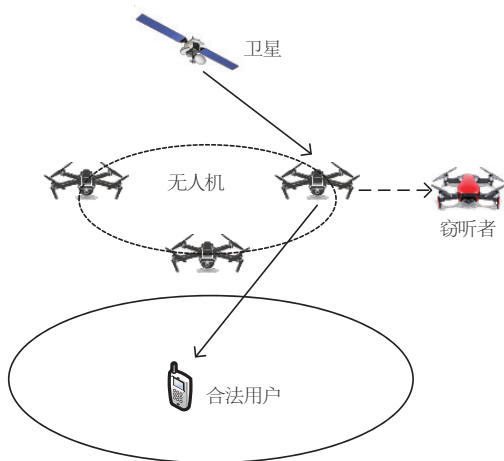


图6 UAV作为中继和窃听者的HSTRN架构

3.3 星地集成网络

目前, 卫星和地面移动系统都在各自的许可频谱上运行, 但现有的频谱分配政策使得卫星的频谱资源日益紧张, 且地面移动系统的频谱得不到充分利用。因此, 频谱拥塞成为卫星和地面协同通信亟待解决的问题。现在的解决方法有两种: 一是开发新的频带; 二是频谱共享, 提高频谱效率。故有学者提出了认知STIN的概念, 保证对现有用户的可接受干扰且动态共享频谱^[13]。概括来说, STIN是为了实现地面、海洋、近地空间和深空各种用户和通信设施之间的高效信息传输和应用共享而提出的架构^[14]。示例如图7所示, 地面网络和卫星网络互相配合, 由一个位于地面上网络控制中心的集中控制模块统一部署, 该模块负责协调频率带宽和系统功率^[15]。参考文献[16]探讨了SOP一定时, 利用卫星和全双工接收机的协同干扰技术, 来使多波束卫星系统的功耗最小化。所提出的基于交替优化的联合波束成形和功率分配算法能够有效降低卫星的功耗, 保证通信系统的物理层安全。

与HSTRN相似, STIN也引入UAV作为可移动的飞行基站, 来提高无线网络的容量, 提供更加便捷高质量的服务。UAV最大的优势就在于, 以其空中自由移动的特性, 可将地面网络、空中网络以及卫星网络通过不同子系统的协作以及多维多模态信息来提供全面而高效的服务^[17]。参考文献[18]采用非正交多址接入 (Non-Orthogonal Multiple Access, NOMA) 将UAV集成到卫星网络中, 使多颗卫星在Ku波段及以上波段合作共同为UAV和移动用户提供高效的服务。在图8所示的场景中, 设计了一种HSTRN架构, 空中的UAV用来海上巡逻、应急响应、通信协助等。参考文献[18]在考虑雨衰效应的前提下, 对一定功率分配概率下的中断概率进行分析, 并提出了一种有效的功率分配算法来解决最小-最大公平性问题, 保障用户的服务质量。

4 现存问题与可行性方案讨论

4.1 现存问题

参考文献[19]提出了对6G的展望, 可视之为后5G时代的研究指南, 其认为, 以人为中心的移动通信仍将是6G最重要的应用。因此, 高安全性、高保密性和高私密性应该是6G的关键特征, 学者应该给予特别关注。在提高6G数据安全性方面, 物理层安全技术和可见光通信的量子密钥分发将发挥重要作用^[20-21]。具体来说, 将这些PLS方法应用到天地一体化信息网络中还存在以下挑战。

首先, CSI对于使用PLS方法的物理层安全性能的设计至关重要。信道的移动性、反馈时延和信道估计误差等因素的影响, 会导致合法通信方无法获取完美的CSI。

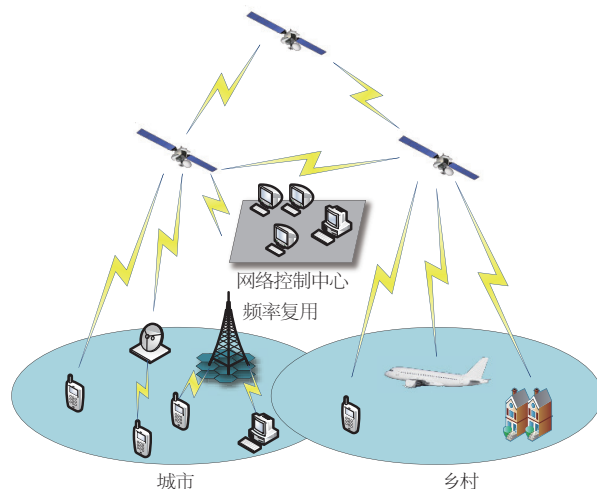


图7 一个典型的STIN架构

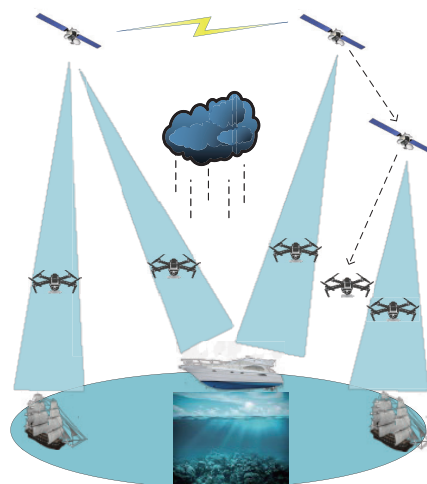


图8 UAV辅助的STIN架构

假设非法用户是被动的, 那么无法获得任何关于窃听渠道的知识。因此, 需要在CSI不完美的条件下设计安全、可靠、健壮通信系统。

其次, 绿色通信和绿色计算已经势不可挡, 特别是在能源有限的天地一体化的物联网场景。很多场景中都在需要传输的信息中添加人为干扰以防止窃听, 然而这种方法不可避免地会带来额外的能源消耗。因此, 在努力提高安全性能的同时, 要考虑能源消耗的问题。

再次, 上述提到的许多物理层安全措施在实践中, 特别是在星地集成网络中, 还没有得到充分的验证。另外, 由于受到许多技术不确定性的影响, 卫星在后5G或6G时代是否能采用PLS方法仍然是一个未知的问题, 还需要更多的工程实践。

此外, 卫星的覆盖范围很大, 可能支持不同类型的

服务。因此,如何满足不同业务对低时延、低成本、数量多等的不同需求是一个关键问题。这样的异构天地一体化信息网络可能会需要PLS措施协同保障安全,而且不同的信道模型可能会使问题更加复杂。

最后,天地一体化信息网络的安全性应该从物理层和物理层上层协同考虑。现有的较为成熟的安全协议大多是针对网络层、应用层而设计的,物理层安全方法只是作为辅助。因此,如何充分利用上层的已有的成熟方案和物理层方法的便捷性是一个重要的课题,可以在未来的研究中加以考虑^[22-23]。

4.2 可行性方案探讨

对于以上所提及的种种问题,本文给出两种可能的解决方式并探讨可行性。

一种解决方案是在现有的星地网络中引入自由空间光通信(Free Space Optical Communications, FSOC),可为地面的短距离通信提供非常高的数据速率,比射频(Radio Frequency, RF)系统支持更多的用户。参考文献[24]在受灾场景下引入可移动式合作中继地面站来提供宽带接入。地面站接收来自卫星的信号,并通过FSOC链路将接收到的信号中继到被屏蔽的目的地。参考文献[25]假设卫星-中继链路服从阴影-瑞利衰落,中继与目的地之间的FSOC链路服从伽马-伽马分布,发现采用AF(Amplify and Forward, 放大转发)中继的混合卫星FSOC系统的分集与FSOC链路的大气动荡参数有关,且最大可实现的分集是由卫星链路决定的。因此,混合星地FSOC协同通信系统不仅经济高效,而且可以较为快速地部署。

但是,鲜有从物理层安全的角度对混合星地FSOC协同通信系统的保密性进行研究。与普通的混合星地通信系统相比,FSOC传播信道在衰落、扰动等方面和RF链路传播特性不同,且FSOC链路的定向性使得窃听者只能从卫星-中继链路接收信号。参考文献[26]混合星地FSOC系统在AF和编码转发(Decode and Forward, DF)两种不同的中继策略下的ASC(Average Secrecy Capacity)和SOP的表达式并进行仿真验证。从而得出结论:对于DF中继策略,保密分集对于合法卫星链路的信噪比为零;对于AF中继策略,保密分集取决于FSOC链路条件和FSOC检测技术。

因此,将FSOC引入现有的天地一体化信息网络,并辅以合适的PLS技术,如编码、密钥生成等,相信对提升网络的安全性和实用性大有裨益。

另一种解决方案是充分利用GEO和LEO各自的优势来提升天地一体化信息网络的物理层安全。GEO位于距

离地面约36 000 km的高空,可用于通信、导航、气象观测等。而LEO位于距离地面300~2 000 km的相对低空,可用于对地观测、通信等。本文汇总的3种天地一体化信息网络的典型架构都是由一颗卫星充当信息发送方,而未将GEO和LEO的优势结合起来形成更加灵活的覆盖方案。相比而言,LEO可通过多颗卫星组网达成全球稳定覆盖,且时延在20 ms以内,上行链路能力远超过GEO的目标。GEO地面终端技术成熟且价格已达到消费级,单星的设计容量大,可弥补LEO利用效率低的缺点。

因此,可让LEO充当星间中继或主动干扰者的角色,将GEO发送的信息进行AF或DF操作后再转发给空中或地面的通信设施。那么,GEO与LEO卫星之间是通过FSOC或RF进行星间链路通信的,而LEO卫星波束小,覆盖范围远比GEO卫星小,本质上降低了被窃听的风险。另外,由于LEO卫星具有移动性,对一般的地面用户来说,过顶时间只有几分钟,不同LEO间的切换可给窃听者带来更多的干扰。故可将本文提到的PLS方法应用到混合GEO-LEO星地网络中,大力提升卫星通信的物理层安全性,为后5G及6G时代的信息传输安全保驾护航。

5 总结与展望

本文首先介绍了天地一体化信息网络的定义及架构组成。其次,阐述了基于信息论的物理层安全技术相比传统加密算法的优点,以及评价系统保密性的主要指标。随后,对天地一体化信息网络的3种不同典型场景LMSN、HSTRN、STIN进行概括,并以UAV作为空中通信设施的代表,研究有无UAV辅助情况下的物理层安全问题。3种场景的优缺点对比见表2。最后,就如何将物理层安全技术实际应用到天地一体化信息网络中需考虑的5点问题进行总结;并提出两种可行性方案,即在现有的星地网络中引入FSOC和构建混合GEO-LEO星地网络。

天地一体化信息网络已成为不可阻挡的发展趋势,天、空、地的恶意窃听者也会一直存在。一方面,当无线信息传输受到不同层级的窃听攻击、干扰攻击、拒绝服务攻击、欺骗攻击、消息伪造等混合攻击时,系统的保密性更加得不到保障,物理层安全的优化和设计将变得更加复杂;另一方面,窃听者如果除了能够发现合法链路的弱点,展开自适应攻击,就会给系统带来致命性打击。因此,针对天地一体化信息网络研究性能良好的物理层安全机制,防御恶意窃听者是一个必将面临的巨大挑战。

参考文献：

- [1] 冯建元,李杰,庞立新,等. 天地一体化信息网络中天基卫星网络架构设计[J]. 电讯技术, 2019, 59(7):775-779.
FENG J Y, LI J, PANG L X, et al. Architecture design of satellite networks in integrated terrestrial-satellite network[J]. Telecommunication Engineering, 2019, 59(7):775-779.
- [2] Li B, FEI Z, ZHOU C, et al. Physical-layer security in space information networks: a survey[J]. IEEE Internet of Things, 2020, 7(1): 33-52.
- [3] SHI Y S, CHANG S Y, WU H C, et al. Physical layer security in wireless networks: A tutorial[J]. IEEE Wireless Communications, 2011, 18(2):66-74.
- [4] BLOCH M, BARROS J. Physical-layer security: From information theory to security engineering[M]. Cambridge: Cambridge University Press, 2011.
- [5] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8): 1355-1387.
- [6] WANG D, BAI B, ZHAO W, et al. A survey of optimization approaches for wireless physical layer security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1878-1911.
- [7] BANKEY V, UPADHYAY P K. Improving secrecy performance of land mobile satellite systems via a UAV friendly jammer[C]//2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). [S.l.:s.n.], 2020: 1-4.
- [8] LI J, HAN S, TAI X, et al. Physical layer security enhancement for satellite communication among similar channels: relay selection and power allocation[J]. IEEE Systems, 2020, 14(1): 433-444.
- [9] LI Y, AN K, LIANG T, et al. Secrecy performance of land mobile satellite systems with imperfect channel estimation and multiple eavesdroppers[J]. IEEE Access, 2019, 7: 31751-31761.
- [10] BHATNAGAR M R, A M K. Performance analysis of AF based hybrid satellite-terrestrial cooperative network over generalized fading channels[J]. IEEE Communications Letters, 2013, 17(10): 1912-1915.
- [11] XU R, GUO D, ZHANG B, et al. Secrecy performance analysis for hybrid satellite terrestrial relay networks with multiple eavesdroppers[C]// 2019 28th Wireless and Optical Communications Conference (WOCC). [S.l.:s.n.], 2019: 1-5.
- [12] 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.
- [13] MALEKI S, CHATZINOTAS S, EVANS B, et al. Cognitive spectrum utilization in Ka band multibeam satellite communications[J]. IEEE Communications Magazine, 2015, 53(3): 24-29.
- [14] YAO S, GUAN J, YAN Z, et al. SI-STIN: a smart identifier framework for space and terrestrial integrated network[J]. IEEE Network, 2019, 33(1): 8-14.
- [15] PENG Y, DONG T, GU R, et al. A review of dynamic resource allocation in integrated satellite and terrestrial networks[C]//2018 International Conference on Networking and Network Applications (NaNA). [S.l.:s.n.], 2018: 127-132.
- [16] GUI G, ZHU Q, XU L, et al. Secure beamforming and jamming for multibeam satellite systems with correlated wiretap channels[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10):12348-12353.
- [17] VONDRA M, OZGER M, SCHUPKE D, et al. Integration of satellite and aerial communications for heterogeneous flying vehicles[J]. IEEE Network, 2018, 32(5): 62-69.
- [18] QI T, FENG W, WANG Y. Outage performance of non-orthogonal multiple access based unmanned aerial vehicles satellite networks[J]. China Communications, 2018, 15(5): 1-8.
- [19] DANG S, AMIN O, SHIHADA B, et al. What should 6G be?[J]. Nature Electronics, 2020, 3: 20-29.
- [20] SHIU Y, CHANG S Y, WU H, et al. Physical layer security in wireless networks: a tutorial[J]. IEEE Wireless Communications, 2011, 18(2): 66-74.
- [21] OBEED M, SALHAB A M, ALOUINI M, et al. On optimizing VLC networks for downlink multi-user transmission: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2947-2976.
- [22] XU N, SUN Y, HUANG B, et al. An energy-efficient cross-layer framework for security in wireless sensor networks[C]// 2011 Fourth International Symposium on Knowledge Acquisition and Modeling. [S.l.:s.n.], 2011: 121-124.
- [23] JI J, LI W, WU B, et al. Design and investigation on image transmission in multi-user cross-layer security network[J]. IEEE Access, 2019, 7: 132066-132073.
- [24] LEITGEB E, SHEIKH MUHAMMAD S, GEBHART M, et al. Hybrid wireless networks combining WLAN, FSO and satellite technology for disaster recovery[J]. Proc. 15th IST Mobile Wireless Commun. Summit, 2005:1-5.

- [25] PETKOVIC M I, PETKOVIC G T, DJORDJEVIC Z M, et al. Analytical approach in evaluation of outage probability of DF based hybrid satellite-terrestrial FSO cooperative system[C]// 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS).[S.l.:s.n.], 2017:326-329.
- [26] AI Y, MATHUR A, CHEFFENA M, et al. Physical layer security of hybrid satellite-FSO cooperative systems[J]. IEEE Photonics Journal, 2019, 11(1): 1-14.

[作者简介]



马方舒（1996-），女，硕士，北京大学信息科学技术学院信息与通信研究所学生，主要研究方向为卫星通信、物理层安全。



王岩（1995-），男，硕士，北京大学信息科学技术学院信息与通信研究所学生，主要研究方向为卫星通信。



张国威（1994-），男，硕士，北京大学信息科学技术学院信息与通信研究所学生，主要研究方向为卫星通信。



程宇新（1974-），男，博士，北京大学信息科学技术学院信息与通信研究所副教授，主要研究方向为卫星通信、物理层安全。