 DOI: https://doi.org/10.12349/iser.v6i8.7041

Discussion on satellite Internet transmission path attack and defense mechanism

Xiong Xiong

Unicom AirNet Co., Ltd.., Beijing, 100032, China

Abstract

With the accelerated global deployment of satellite internet, securing transmission paths has become a critical component of system security. Given the characteristics of massive constellation scales, frequent topology changes, and open links in satellite networks, various threats such as signal interference, man-in-the-middle attacks, node denial-of-service (DoS) attacks, and routing spoofing frequently occur during data transmission. To address these challenges, this paper proposes a multi-layered defense strategy from four perspectives: physical layer, link layer, network layer, and cross-layer collaboration. The approach integrates signal anti-interference and spectrum scheduling, blockchain-based distributed verification, advanced self-healing mechanisms, quantum communication protection, layered link encryption, and dynamic key management. Only through simultaneous implementation of these technologies across multiple layers can we ensure stable and secure satellite internet transmission in complex constellation operation environments.

Keywords

satellite internet; transmission path; security; attacks; defense mechanisms; research

卫星互联网传输路径攻击及防御机制探讨

熊雄

联通航美网络有限公司，中国 · 北京 100032

摘　要

目前全球范围内建设卫星互联网步伐加快，其传输路径安全成为体系安全的关键一环。由于体系存在着星座量级巨大、拓扑变化频繁、链路开放等特性，在传输中易出现信号干扰、中间人链路篡改、节点拒绝服务以及路由欺骗等不同类型威胁。面对该现状，本文基于物理层、链路层、网络层和跨层协同四个角度，提出了包括信号抗干扰及频谱调度、区块链分布式验证、前沿自愈及量子通信防护和分层链路加密及动态密钥管理机制在内的多层次防御思路。唯有在多层面上同时开展相关技术部署才能确保卫星互联网传输在复杂星座运行环境中的稳定与安全。

关键词

卫星互联网；传输路径；安全；攻击；防御机制；探讨

1 引言

卫星互联网具有覆盖广、链路通达、接入灵活的特点，因此在新一代全球信息基础设施中占据着较为重要的地位。与地面网络相比，利用卫星通信需要经过多个环节的传送（跨越卫星星座、星间链路以及地面网关），并且链路上存在多节点、多地域的交互协作，因此需要从物理层到应用层全方位结合卫星通信的特殊环境考虑安全防护体系的构建。

2 卫星互联网传输安全现状

卫星互联网的全球覆盖及高速接入需求推动了行业快速发展，然而传输安全风险也逐渐凸显。第一，链路处于外层空间和大气层中，因此很容易被电磁干扰、空间辐射等所破坏，造成链路信号衰减不稳定。而且会受到射频干扰以及黑客恶意攻击，在个别地区已经发现用定向干扰设备扰乱卫星链路信号的情况。第二，因为卫星互联网的开放特性，在数据交互的过程中很容易发生被窃听、截获的情况，而且链路经过了卫星、地面站、用户终端等多个点位，在管理过程中安全性要比传统通信网络更难，可能会发生中间人篡改信息的问题，导致数据完整性的失效 [1]。第三，卫星互联网是大量、多节点、具有动态拓扑结构的网络，在路由协议的频繁跳转的过程中，这些信息都很容易被伪造或者篡改，由此便容易造成路由欺骗或者链路劫持。第四，当网络规模越来越大时，遭受拒绝服务攻击以及出现异常流量集中的可能性就会增大，有可能会出现某一部分地面站或者卫星节点因为处理能力有限而导致整个链路产生故障连锁反应，从而影响到整体的传输安全性。

【作者简介】熊雄（1980–），男，中国湖南浏阳人，硕士，工程师，从事卫星互联网系统建设和维护，卫星互联网络安全风险和防范研究。

3 卫星互联网传输路径安全防御的重要性

卫星互联网的传输路径安全防御在整个通信体系中占据重要的地位。一方面因为卫星链路覆盖面积广，节点相对密集，任意一点出现问题都会造成大范围的通信受影响。所以建立起完善的防御，避免因为一个小链路故障让整个系统瘫痪的情况发生，保证跨区域间数据通信的稳定。另一方面，卫星互联网包含了军事、能源、金融以及公共服务业等领域的大规模数据传输，如果传输路径不加以保护，极有可能被人利用来窃取机密，从而产生严重的后果。保护传输路径不仅是要保护所拥有的重要资料完整且不可篡改，在途中不受任何攻击和阻挠，还在于保证在复杂环境下核心业务得以持续运转。不仅如此，面对低轨卫星组网过程中节点数目的不断增多和拓扑结构变得越来越复杂的情况，频繁发生路由切换、链路调度，容易引发如拒绝服务攻击、链路劫持等新型攻击。为了应对突发性的攻击，需要在不同的层面上建立起多层面的安全防护体系，使其拥有更大的容错性，提供更强的网络健壮性和自适应性 [2]。

4 卫星互联网传输路径攻击

4.1 信号干扰攻击

信号干扰是卫星互联网的一大安全问题。因为卫星链路主要是凭借射频信号来实现大面积覆盖，攻击者如果使用高功率发射机便可以造成长时间带宽噪声，导致卫星链路接收端信噪比降低，链路误码率增大甚至无法正常传输信息。而且攻击者使用定向干扰设备可以在某个时段内对该卫星或者地面站的指定频段进行集中辐射，造成目标卫星或者地面站的通信能力下降甚至完全丧失，除此之外，欺骗式干扰是更为复杂的干扰方式，攻击者通过对信号特征进行模拟，使接收端对解调和同步产生错误判断，造成传输链路异常。当前干扰手段也越来越智能化，攻击者能够利用频谱感知设备去寻找容易被攻击的频段，并有针对性地加以打击，大大增加了链路抗干扰保护的复杂度。

4.2 中间人链路篡改

中间人攻击发生在数据传输期间，攻击者隐匿于卫星转发节点或者地面站链

路上截获并更改伪造的数据包。其中篡改方法不仅仅是篡改数据内容，还包括数据重放以及伪造身份认证，使得通信双方无法识别数据信息的真实情况。此类攻击比较隐蔽，不易被察觉，一般不会直接破坏链路传输，而是通过长期潜伏窃取信息或是渐进式地降低链路传输可靠度 [3]。有的攻击者甚至利用链路加密和密钥管理方面的缺陷，通过得到加密材料来读取数据内容。由于卫星互联网规模庞大，一部分低级别的卫星互联网结点防护薄弱，而成了中间人攻击的重点对象。

4.3 节点拒绝服务攻击

拒绝服务攻击以破坏卫星或者地面站节点处理能力为出发点，攻击者采用大量异常请求或流量灌入手段，迅速耗尽节点资源，使得正常用户不能获取服务。如在大尺度星座组网系统中某一点出现故障，就会凭借网络的连通性与连锁反应导致局部网络失效。分布式拒绝服务攻击（DDoS）则是通过多处攻击源同时向目标系统发动进攻行为的攻击方式，将会给系统带来更多危险，除了可以造成较大的传输时延和路由失效外，还可能会造成协议漏洞滥用下的低流量慢速攻击以达到永久占据用户节点资源的目的。在资源受限的卫星系统中，该种攻击可能会发挥出更大威力。

4.4 路由欺骗与伪装攻击

路由欺骗攻击就是利用卫星互联网动态拓扑的特点，篡改或伪造路由信息，让数据包偏离原先设定的路径，或者诱导数据绕行至攻击者自身所控制的恶意节点处，并对其进行窃听、篡改或删除等操作，以达到破坏链路完整性的目的。伪装攻击是冒充合法节点参与网络路由更新，将错误的拓扑结构信息注入路由中，从而导致路由形成环路或某一路由出现拥塞的情况。卫星互联网采用的是频繁切换链路规划的方式，所以路由欺骗可以很快地影响大量节点。除此之外，有些攻击者会使用路由欺骗加中间人手段，以完全控制传输数据，导致系统风险不断加剧。此类攻击除了会降低通信效率外，也会导致大量的传输中断。

5 卫星互联网传输路径防御机制探讨

5.1 信号抗干扰与频谱调度

卫星互联网传输易受地面或空间的干扰源影响，为了保持链路稳定，必须建立抗干扰和频谱调度的机制。首先，从物理层面上，可使用波束赋形技术来调整天线阵列的方向图，使得天线阵列对准目标区域、天线阵列方向图上的信号能量被集中到目标区域，有效地降低非目标区域内的辐射能量，并且抑制了干扰源对于链路的影响程度。另外，MIMO 结构在接收端将采集到的不同路径信号合成处理，提高了信噪比降低了误码率，提供更强的鲁棒性。其次，可通过频谱动态调度方法来缓解强干扰情况下的不利影响，借助认知无线电感知外部频谱环境的变化，捕捉干扰源的频段以及功率特性，并据此对发送信道做相应的调节，以此来获得灵活的频谱迁移策略。再者，在协议层及物理层对接方式中形成抗干扰机制，在设备接收到的数据存在干扰时，快速响应链路工作情况的变化，自主地通过改变自身的调制级数或纠错编码强度去提高系统的抗干扰能力。通过多层的抗干扰加频谱调度会为整个星座组网链路提供更加安全可靠的保障 [4]。

5.2 区块链与分布式验证机制

基于区块链技术的卫星互联网多节点传输，通过利用区块链特点使路径更加安全和透明。首先，由于区块链是去中心化的，不存在某一点控制网络的行为，所以在保证链路连接时也可以排除路由伪造，或者是链路篡改现象的发生。利用分布式的账本可以达到全网节点同步更新链路的状态

信息，并且各节点能对应传输路径的一致性进行检验，防止恶意节点伪造数据包或者篡改路由表。其次，基于，智能合约实现卫星链路的接入与切换过程的自动验证，当节点接入卫星互联网的时候需要满足合约要求的条件才可以进行网络接入，未经授权者一律禁止接入。这一机制相较于传统集中认证方式来说，其更为适用于大规模组网或者拓扑变更较大的情况，能够保证认证实时性，并且不能更改。再者，应用区块链共识算法有效确保卫星互联网数据的一致性。即使有一些节点早手工艺或是出现异常，也能够通过拜占庭容错，权益证明或是混合共识等机制来保证链路的状态信息正确，可以避免恶意节点用虚假的信息引导数据路径偏离既定轨迹，对于动态路由更新非常关键。此外，应用分布式验证机制来多层次监控链路传输，每一节点进行数据包转发时的传输轨迹均会被记录下来，利用哈希函数实施加密标记，这样在后续验证过程中一旦出现篡改行为均会被及时辨识出来。这种不可逆的记录方式可以确保数据回溯，并给后续攻击追踪与取证提供信息依据。

5.3 前沿自愈与量子通信防护

对于大规模的卫星群，引入自愈机制能够在链路遭受攻击之后及时恢复效率。系统通过对链路状态进行实时监测，一旦发现异常能够在短时间内切换到备用线路，同时使用在较短时间内重新规划出一条临时性的备用路径，采用跨节点方式来躲避局部失效对整体网络的冲击。自愈机制需要依靠一定的冗余路由资源进行，需要使用机器学习的方法对异常模式进行识别和预测，在攻击尚无扩大蔓延的情况下就进行路径调整，真正做到动态适应，有效防守。此外，量子通信能使传输路径的安全等级得到进一步提升，通过对链路的加密采用量子密钥分发方法，应用量子态不可克隆及测量塌缩特性，保证在交换密钥环节不会发生窃取或复制的问题。通过有效结合自愈和量子防护可以为卫星互联网构建起从攻击检测到路径修复再到密钥保护的多维防护，有效提升传输路径的韧性和安全性。

5.4 分层链路加密与动态密钥管理

在卫星互联网传输链路上实施分层链路加密，保证不同链路等级具有相应的防护级别。在卫星互联网传输链路上实现分层链路加密，不同的链路等级有不同的防护级别，例如：在物理层可采用信号加扰、低概率截获编码技术等防止链路被外部窃听；在数据链路层采用分组加密技术使得每一个帧都拥有独立的保护属性，即使某个中间节点失陷也不会导致更大范围的信息泄露；在网络层通过使用端到端的加密协议来保证流经该层所有节点的数据内容都是保密的。不同层次的加密相结合可以保障在攻击者成功突破某一层次防护的情况下，也能够有效保护链路整体的安全。除此之外，动态密钥管理也是防止密钥泄露和破解的关键措施，采取基于时间片的密钥更新方式，可以在很短的时间范围内自动生成与分发新的密钥，将攻击者已窃取密钥的有效时间缩短。此外，还可将会话密钥机制应用到卫星节点链路切换过程中，在每个通信阶段分别生成一组临时加密参数，这样就增加了数据通信的不可预测性，同时密钥分发也可以借助分布式节点之间协作来避免某个单点密钥服务器遭受攻击。

6 结语

总而言之，过去单一的防护手段已无法满足越来越复杂的卫星互联网传输安全问题，而如何整合跨层跨域的防守机制是解决这一问题的关键所在。基于此，以信号的安全传输途径入手，分析信号遭受的多方面攻击方式和影响（信号干扰、中间人篡改、节点拒绝服务、路由欺骗等），然后从安全防护的角度出发，提出频谱调度和抗干扰、区块链分布式验证、量子通信和自愈机制、分层链路加密和动态密钥管理等解决方法，以此形成有效的跨层维度自适应安全防护能力。

参考文献

[1] 谷欣,单超,孙才俊,等.卫星互联网安全风险及应对措施分析[J].天地一体化信息网络, 2024, 5(1):95-101.

[2] 张元玉,赵双睿,何吉,等.卫星互联网安全:需求,现状与趋势[J].网络空间安全科学学报, 2024, 2(4):2-17.

[3] 王逸璇,李洋,杨皓琪,等.面向卫星互联网的链路层加密系统设计[J].网络空间安全科学学报, 2024, 2(4):95-105.

[4] 孙茜,刘慧梁,王冀莲.卫星互联网信息安全风险分析与发展建议[J].中国电子科学研究院学报, 2023, 18(5):469-475.