

低轨卫星网络星间路由安全机制研究

薛文浩¹, 潘恬¹, 卢诚承¹, 杨帆¹, 黄韬^{1,2}, 刘韵洁^{1,2}

(1. 北京邮电大学网络与交换技术国家重点实验室, 北京 100876;

2. 网络通信与安全紫金山实验室, 江苏 南京 211111)

摘要: 为了保障路由的安全性和抗毁性, 设计面向星间路由的安全机制和故障恢复机制成为维护低轨卫星网络可靠通信的关键。为了应对卫星网络可能面临的安全威胁, 分析不同路由攻击行为对典型星间路由协议的影响, 并设计差异化的协议包安全认证机制和链路故障恢复机制。此外, 搭建基于虚拟化技术的卫星网络仿真平台, 通过仿真多种路由攻击场景, 验证所设计星间路由安全机制的有效性, 并评估引入安全机制前后的 CPU 占用率、协议包处理时间等性能指标。实验结果表明, 在有限的认证时间和路由开销下, 该星间路由安全机制能够有效防范空间网络环境中的多种安全威胁, 并减少由突发链路故障引起的通信时延, 从而保障低轨卫星网络的安全可靠通信。

关键词: 低轨卫星网络; 路由协议; 路由安全攻击; 链路故障恢复; 安全攻击仿真

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2023015

Research on LEO Satellite Network Routing Security

XUE Wenhao¹, PAN Tian¹, LU Chengcheng¹, YANG Fan¹, HUANG Tao^{1,2}, LIU Yunjie^{1,2}

1. State Key Laboratory of Networking and Switching Technology, BUPT, Beijing 100876, China

2. Purple Mountain Laboratories, Nanjing 211111, China

Abstract: The design of secure mechanisms and failure recovery mechanisms for inter-satellite routing has become pivotal in maintaining dependable communication within the LEO satellite network. To address the potential security threats faced by satellite networks, the impact of different routing attack behaviors on a typical inter-satellite routing protocol was analyzed and differentiated packet security authentication mechanisms and link failure recovery mechanisms were designed. Additionally, a satellite network emulation platform based on virtualization technology was constructed, enabled the verification of the effectiveness of the designed inter-satellite routing security mechanisms through the emulation of various routing attack scenarios. Furthermore, performance metrics such as CPU utilization and packet processing time were also evaluated before and after the introduction of security mechanisms. Experimental results demonstrated that the proposed inter-satellite routing security mechanism effectively mitigated multiple security threats in the space network environment while reduced communication latency caused by sudden link failures, thereby ensured secure and reliable communication within the LEO satellite network.

Keywords: LEO satellite network, routing protocol, routing security attack, link failure recovery, security attack simulation

0 引言

近年来, 随着 SpaceX 等公司采用大规模低轨卫星星座构建卫星互联网^[1-2], 低轨卫星网络正加速成为建设空间信息网络的重要组成部分。其中, 星间路由作为卫星网络

通信的核心底层技术, 决定着星间组网及星上数据传输的高效性和可靠性。由于低轨卫星网络存在通信场景开放、网络拓扑时变等特点, 路由协议在星间链路切换时会产生较多的路由协议包^[3-4], 在复杂的空间网络环境下极易受到恶意卫星的干扰攻击, 这将影响星间路由的稳定性, 甚至

收稿日期: 2022-12-30; 修回日期: 2023-05-10

通信作者: 潘恬, pan@bupt.edu.cn

基金项目: 国家重点研发计划资助项目 (No.2018YFB1800602, No.2019YFB1802600)

Foundation Items: National Key Research and Development Program of China (No.2018YFB1800602, No.2019YFB1802600)

威胁卫星网络安全。因此,调研并仿真低轨卫星网络中的多种路由攻击场景,分析不同攻击行为对星上通信造成的影响,并针对攻击行为设计安全防护机制具有重要意义。

针对卫星网络的路由攻击主要包括伪造节点身份后实施的干扰、篡改、重放行为以及针对报文数据的窃听攻击,将引发路由中断、路由黑洞、路由信息泄露等一系列问题。参考文献[5]引入基于信誉度的安全识别机制,将实时路由行为作为量化卫星信誉度的指标,并把信誉度较低的卫星隔离,避免该卫星对星间路由造成影响。参考文献[6]将转发数据量作为卫星信誉度的量化指标,将数据量转发过低的卫星排除在正常转发路径之外。参考文献[7]将基于信誉度的安全认证机制引入多层卫星网络,防范信誉度过低卫星节点的潜在威胁。然而,上述工作需要经历多次路由攻击后才能量化卫星信誉度,无法主动预防各种路由攻击行为。同时,将转发数据量作为卫星信誉度的量化标准,忽略了低轨卫星网络拓扑频繁变化对卫星信誉度造成的影响。参考文献[8]提出一种采用证书的层次式路由认证协议,在路由初始化时卫星节点首先获得合法的证书,在路由建立过程中每个节点对证书进行核验。其不足之处在于该类协议无差别地对所有协议包采用相同的认证机制,从而增加了分布式路由处理的开销。考虑到不同攻击场景下路由安全需求并不一致,需要针对不同安全威胁设计差异化的路由安全认证机制。

卫星网络发生软硬件故障或遭受路由攻击时可能导致通信业务中断,因此快速再寻路机制对于减少业务中断时间、确保星上业务的连续性非常重要。根据故障发生位置,卫星网络故障可分为卫星节点故障和星间链路故障两种。卫星节点故障意味着故障卫星与邻居卫星之间所有链路的中断,因此可以将卫星网络故障研究简化为对星间链路故障的研究。目前,星间链路故障的研究主要集中在故障链路预测机制^[9-10]和利用替代路径转发原故障链路流量^[3-4, 11]两个方向。传统的星间链路故障再寻路方案借鉴了地面网络的动态路由协议,故障链路信息需要进行洪泛广播^[3-4]。由于未限制洪泛区域,故障信息需要洪泛至全网,造成星上带宽资源的过度占用并进一步增加路由收敛时间,且面对巨型星座时方案不具备可扩展性。因此,如何有效降低故障发生时的路由洪泛开销,同时压缩故障恢复时间以确保业务连续性值得深入研究。

针对低轨卫星网络中存在的多种安全威胁,本文基于经典的动静结合低轨卫星路由协议 OPSPF^[3],提出一种星间路由安全机制,根据路由更新时产生协议包的种类、用途以及面临的安全攻击行为,为不同报文设计差异化的认

证防护方法。同时,针对卫星网络的突发故障,设计基于故障信息局部洪泛的快速再寻路机制,通过为协议包选取局部最优洪泛路径减少路由收敛时间,以减少故障链路对星上通信业务的影响,提高星间路由的自愈能力。此外,本文还搭建了网络协议仿真平台对上述协议设计的有效性进行验证。

1 背景及相关工作

1.1 星间路由协议

相较于中高轨卫星网络,低轨卫星网络具有通信时延低、信号覆盖面广、路径冗余度高等优点。另外,低轨卫星网络中卫星分布密集,星座拓扑结构复杂,星间链路切换频繁,实现全网路由收敛需要更多且更复杂的协议包交互,这对有限的星上计算/存储资源、星间链路带宽资源提出了挑战,也为星间路由安全带来了潜在威胁。当前学术界提出了多种适用于低轨卫星网络的路由协议。

(1) 基于卫星位置推算的数据包路由算法^[12]实现了一种静态分布式路由协议。卫星节点在收到数据包后根据当前时刻节点位置对星间网络拓扑状态进行建模,根据推算的卫星位置关系计算数据包下一跳的最优转发路径。其不足之处在于面对突发故障引起的拓扑变更时,卫星节点无法及时感知链路状态。

(2) 星座快照路由协议^[13]根据低轨卫星网络拓扑规律变化的特点,将星座拓扑变化切分为有限的拓扑状态集合,当时间片足够小时卫星网络拓扑固定不变,从而将卫星拓扑变化建模为有限状态机。在每个时间片内卫星节点根据当前网络拓扑状态,利用最短路径算法更新该状态下的路由表项。该星间路由协议同样不能根据链路状态突发变化动态更新路由,不具备网络抗毁性。

(3) 链路定向探测星间路由协议^[14]利用星座拓扑变化的规律性,对即将发生通断变化的链路发送报文进行定向探测,并在链路变化后进行链路状态同步及路由表项更新,从而消除快照序列的存储开销,同时降低全网链路探测引起的通信开销。但该协议同样无法快速感知网络突发故障引发的链路状态更新,网络抗毁性能有待提高。

(4) 基于软件定义网络的星间路由协议^[15]将软件定义网络架构^[16]引入卫星网络,将地面站作为控制器向卫星节点下发流表,保证对路由的集中式控制,从而使卫星网络具备可编程性。然而,考虑到星地拓扑的高动态性,基于频繁切换的星地链路构建稳定的控制通路面临较大的挑战。此外,软件定义的集中式控制通常存在控制器单点故障的可靠性问题。

(5) 基于动静结合的星间路由协议^[3]根据星间网络拓扑规律变化、星间链路不稳定的特点,将快照路由由协议与链路动态探测相结合:对于规律性星座拓扑变化,采用静态快照路由协议更新路由,减少星上资源损耗及链路探测带来的通信开销;对于可能出现的链路突发故障,采用链路动态探测机制实时感知链路状态变化,并按需进行链路状态变化全网洪泛,从而增强网络抗毁性能。

1.2 卫星网络安全攻击行为

网络安全性是确保通信服务安全稳定以及用户隐私数据不被泄露的关键。卫星网络面临各种攻击,这些攻击主要通过影响通信数据的完整性、机密性和通信系统的可用性来威胁网络安全。常见的攻击方式包括以下几种^[17-18]。

(1) 窃听攻击:在通信网络中,如果数据未经过加密或者加密强度过低,攻击者可以通过监听通信网络中的数据并破解密钥,从而影响信息传输的机密性。恶意节点可以窃听用户传输的信息,导致隐私数据泄露。此外,恶意节点还可以针对协议报文进行窃听,获取系统信息和路由控制信息,并在此基础上对数据进行伪造攻击,给网络安全带来威胁。

(2) 伪造攻击:当通信流程中缺乏严格的身份认证机制时,恶意节点通过伪造合法身份接入通信网络,并发送伪造报文,将伪造后的数据插入正常数据中传输,影响数据完整性。当所伪造的信息为系统信息或路由控制信息时,伪造报文会影响通信系统可用性,造成网络瘫痪。

(3) 篡改攻击:恶意节点在截获通信数据后,可能会对用户信息进行篡改,从而影响传输内容的完整性;或者会篡改系统信息,导致通信系统的可用性受到影响,进而引发网络瘫痪。此外,恶意节点还可能在截获通信数据后,间隔一定时间后将报文再次注入网络,造成网络瘫痪。

(4) 黑洞攻击:也叫封包丢弃攻击,是指恶意节点在通信过程中截获数据包后,故意拒绝服务并丢弃这些数据包,从而导致网络瘫痪或服务中断的攻击行为。

2 星间路由安全机制设计

2.1 安全需求分析

鉴于参考文献[3]中提出的基于动静结合的星间路由协议 OPSPF 具备多种优势,既能有效利用星座拓扑变化规律,避免不必要的故障状态同步,又能在突发故障发生时通过链路探测和按需全网洪泛实现快速路由收敛。因此,本文选择 OPSPF 作为研究对象,分析该协议可能面临的安全威胁,并针对不同的路由攻击场景设计差异化的

安全认证机制。

针对低轨卫星网络的规律性拓扑变化,OPSPF 采用基于快照拓扑切片的静态路由更新机制。卫星节点通过推导全网拓扑状态,通过本地计算确定数据包的最优转发路径并更新路由表,此过程无须协议包交互,因此恶意节点无法干扰路由更新。为应对突发性链路故障,动态路由机制融合了地面网络的开放最短路径优先(Open Shortest Path First, OSPF)路由协议的泛洪机制,并优化了信令开销。卫星节点周期性发送 Hello 探测报文以感知链路状态,并在突发链路状态变化时通过全网洪泛的链路状态更新(Link State Update, LSU)报文同步卫星节点的链路状态数据库并更新路由。恶意节点主要通过干扰、欺骗和篡改这些协议包来进行路由攻击。图1为基于动静结合的星间路由协议 OPSPF 的动态路由更新流程示意。

根据动态路由更新机制中协议包的作用不同,针对协议包的路由攻击主要包括以下几种。

(1) 窃听攻击:攻击卫星通过窃听当前网络中路由协议所携带的信息,分析当前链路状态及路由代价,造成网络拓扑结构、星间链路状态等信息的泄露,并可在窃听的基础上对数据进行伪造,给路由安全带来威胁。例如,攻击卫星可以窃听 LSU 协议包,分析当前星间网络拓扑状态,给路由安全带来威胁。

(2) 伪造攻击:恶意节点通过发送伪造的路由控制信息影响路由安全。攻击卫星可以伪造 Hello 探测报文,并定时向故障链路两侧端口发送,影响卫星节点对链路状态的正确感知,造成路由始终不收敛。攻击卫星也可以伪造 LSU 协议包,将虚假的链路更新信息注入卫星网络。在虚假的链路更新信息未传递到所描述的更新节点时,其他节点不能对这一信息的真实性进行查核,将继续洪泛该伪造的 LSU 协议包,这将造成无效的协议包洪泛及错误的路由更新,引发通信业务中断及错误路由更新的额外开销。

(3) 篡改攻击:恶意节点通过篡改卫星网络中正常的路由控制信息影响路由安全。例如,攻击卫星通过截获后篡改或延迟发送网络中正常传输的 LSU 协议包,导致 LSU 报文的链路更新信息错误或过期发送。其他节点收到被篡改或延迟发送的 LSU 报文后将错误地更新本地链路状态数据库及路由表,并继续对该 LSU 协议包进行洪泛,直到传递至描述端口所在卫星节点时才能对链路更新信息的正确性进行查核。这将造成错误或过期的协议包在卫星网络中洪泛,中断正常的通信业务并带来错误路由更新的额外开销。

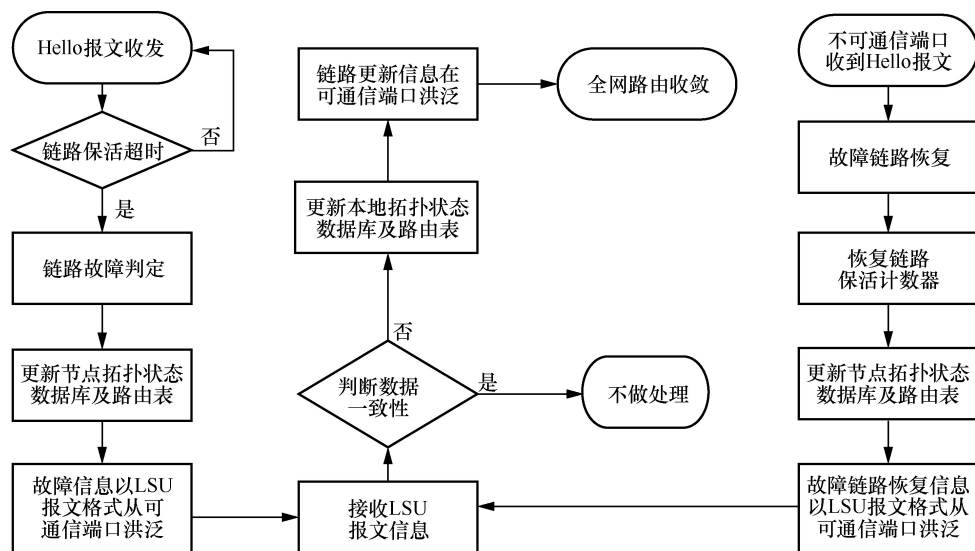


图1 基于动静结合的星间路由协议 OPSPF 的动态路由更新流程示意

(4) 黑洞攻击: 恶意节点通过截获并丢弃特定的路由控制信息影响路由安全。例如, 攻击卫星截获后丢弃星间链路上正常的 Hello 探测报文, 造成星间链路的“假中断”, 引发不必要的链路状态全局洪泛, 造成宝贵的星上计算资源和星间链路带宽的浪费。

2.2 报文安全认证机制

2.2.1 报文完整性保护流程

报文完整性保护指信息传递过程中需要保证接收端接收到的数据与发送端一致, 数据不因恶意攻击行为受到篡改或损坏。对协议报文的完整性保护主要通过报文摘要算法实现, 完整性保护流程如下。

(1) 消息发送处理: 发送端认证密钥与报文数据经过报文摘要算法计算后, 得到唯一的报文鉴别码 HMAC, 附加在报文后一起封装在数据包中。发送节点发送报文时将鉴别码附加在报文后一并向下一节点传送。

(2) 消息接收处理: 接收端收到数据包后, 首先查看数据包中是否包含报文鉴别码 HMAC, 从而判断是否进行消息认证及完整性保护。对于未包含报文鉴别码的数据包, 无法验证报文来源及数据完整性, 不对该数据包进行处理。随后, 接收节点利用本地认证密钥及报文摘要算法执行运算, 并将新生成的报文鉴别码 HMAC 与数据包中附加的鉴别码对比。由于报文摘要算法主要由单向散列函数实现, 同一数据经过相同散列函数计算后只会生成唯一的密文, 且无法进行逆运算。消息接收端与发送端保存有相同的报文摘要算法及本地密钥, 对报文执行两次摘要算法得到的报文鉴别码 HMAC 相同。若报文由可信任节点发送且中途未被篡改, 生成的报文摘要将保持一致; 若报

文中途被篡改或损坏, 接收节点生成的摘要将与原始的鉴别码不一致, 从而可以验证报文的完整性。

2.2.2 报文机密性保护流程

在保证报文完整性的基础上, 还需要保证部分报文的机密性, 防止数据被窃听造成的隐私泄露及系统威胁。在数据通信过程中, 报文的防窃听机制主要由加密算法实现。运行星间路由安全机制的发送节点在发送协议包时, 首先根据协议包种类判断是否需要为报文引入防窃听机制。对于需要进行机密性保护的报文, 通过本地密钥及加密算法将报文数据转换为密文在网络中传送。接收节点收到协议包后, 使用解密密钥对协议包中的密文进行解密运算, 得到可读的明文数据, 再利用协议包处理逻辑对报文明文数据进行处理。报文转换为密文传送后, 即使密文被截获, 由于恶意节点未保有相应加密算法及密钥, 无法窃听协议包内容, 从而实现消息的机密性保护。

2.2.3 差异化安全认证机制

基于星间路由协议中两种报文的不同安全需求, 分别设计报文认证及报文加密两种安全防护策略。其中, Hello 报文不携带关键路由控制信息, 因此只需要利用认证机制对报文来源及完整性进行验证; LSU 报文携带链路状态变化及路由控制信息, 因此既需要利用认证机制对协议包来源的合法性及完整性进行验证, 以应对针对报文的篡改及伪造攻击, 同时也需要利用加密算法对协议报文进行机密性防护, 以防止路由信息被其他恶意节点窃听。

对 Hello 协议包及 LSU 协议包进行来源认证及完整性保护时, 可以通过报文摘要算法生成唯一的报文鉴别码 HMAC, 与报文内容一起封装在数据包中传送。接收端收到

数据包后,将报文数据取出,通过本地摘要算法生成新的鉴别码,并与收到的报文鉴别码进行比对,若匹配就验证其报文完整性及来源合法性,否则丢弃该数据包。对 LSU 报文进行机密性保护时,可以利用对称加密体系在星间链路两侧分别对报文数据执行加解密算法,确保报文数据转换为密文在卫星网络中传递,恶意节点即使截获 LSU 协议包仍无法正确解析报文数据,从而实现协议包防窃听机制。图 2、图 3 分别为针对 Hello 报文及 LSU 报文的加密认证机制。

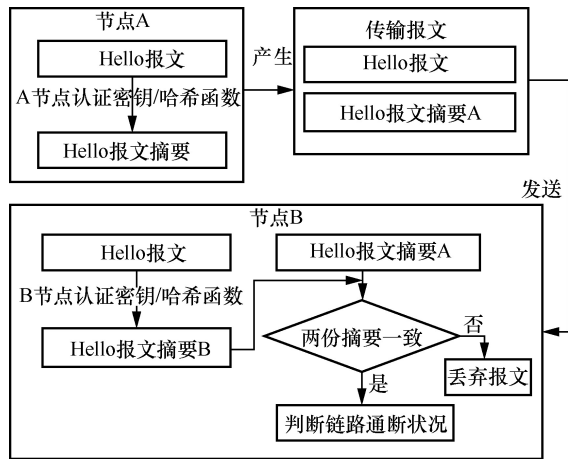


图2 针对 Hello 报文的加密认证机制

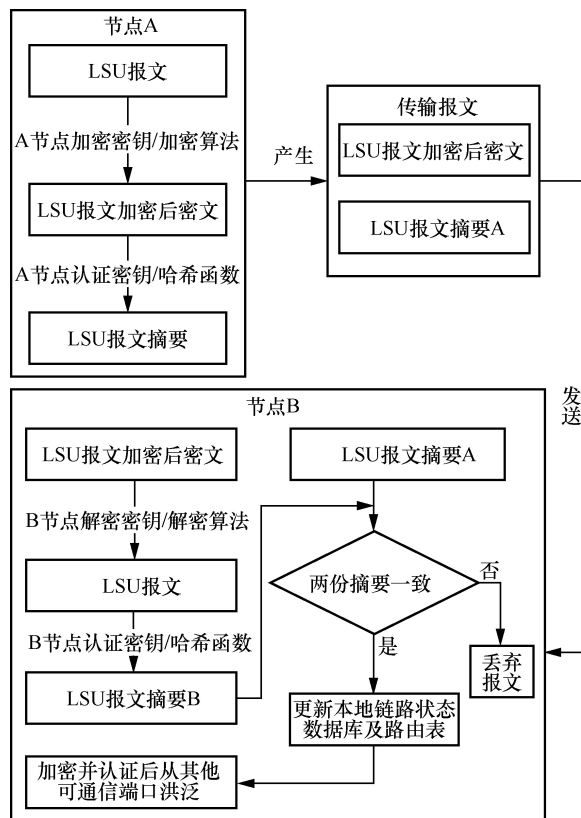


图3 针对 LSU 报文的加密认证机制

2.3 链路故障再寻路机制

星间路由协议加入安全认证机制后,能够防范对协议包的伪造、干扰、欺骗行为。除此之外,考虑到低轨卫星网络处于复杂的空间环境,物理设备或链路的突发故障不可能完全避免,因此,需要设计一套针对低轨卫星网络的星间链路故障快速再寻路机制,为经过故障链路的数据包快速寻找一条替代转发路径,保证星上业务的连续性。针对突发链路故障问题,传统方法基于星间动态路由协议将故障信息在全网洪泛,以实现全网路由收敛。然而,这会产生大量的路由协议包,占用宝贵的卫星网络带宽资源。本文根据低轨卫星网络拓扑结构链路高冗余度的特点,提出一种基于局部洪泛思想的链路故障再寻路机制,为经过故障链路的数据包快速生成替代转发路径,且基于局部洪泛的故障再寻路开销极低。

保证星间通信可靠性的链路故障快速恢复机制流程如下:当发生星间链路故障时,故障链路两侧卫星使用最短路径算法计算当前故障链路的最优替代转发路径,同时将链路故障信息定向洪泛至转发路径上的各节点,更新转发路径上节点的链路状态数据库及路由表。考虑到卫星网络拓扑的高冗余度,当某条星间链路发生故障时,连接故障链路两侧卫星节点的最优替代路径并不会过多地“绕远”,且故障链路局部区域以外的路由通常不会产生剧烈变化。因此,以上局部洪泛思路仍然能够保证端到端链路的可达性,且替代路径的端到端距离不会偏离原来的最短路径太多,但却消除了全网洪泛故障信息的巨大开销。

当已经发生星间链路故障的卫星再次发生链路故障时,计算得到的最优替代路径将有可能经过原故障路径,且该节点附近存在恶意节点的概率较大,不再适合采用局部洪泛策略以较低代价计算报文的替代转发路径。此时,链路故障快速恢复机制将回退到故障信息全局洪泛的状态并将链路故障情况向地面控制中心通报。考虑到卫星节点发生二次故障的概率较低,以上回退机制仅在较小概率情况下被触发。图 4 为链路故障快速恢复机制的完整处理流程。

图 5 通过一个例子更好地说明基于局部洪泛的链路故障快速恢复机制。在该示例场景下, SAT1 节点向 SAT12 节点发送数据包,初始情况下的转发路径为: SAT1-SAT2-SAT6-SAT7-SAT11-SAT12。在某个时刻, SAT6 与 SAT7 节点间链路发生了故障,此时如果将该故障信息向全网洪泛则会占用较多的网络带宽资源和星上处理资源。假设发生故障后, SAT6 和 SAT7 节点通过最短路径计算得到的替代转发路径为 SAT6-SAT10-SAT11-SAT7。此时

可以定向更新该替代路径经过节点（即 SAT6、SAT10、SAT11、SAT7）的链路状态数据库及路由表。最终，SAT1 发送的数据包将通过完整的端到端替代转发路径 SAT1-SAT2-SAT6-SAT10-SAT11-SAT12 发送至 SAT12 节点。综上，在当前 SAT6 节点只存在一条故障链路的情况下，局部洪泛策略可以为经过故障链路的数据包快速寻找替代路径，且将链路故障的洪泛影响限制在局部区域，不会耗费过多的网络资源。

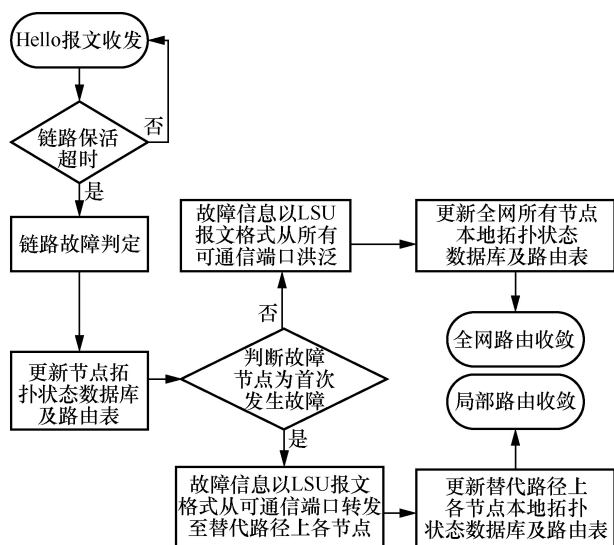


图4 链路故障快速恢复机制的完整处理流程

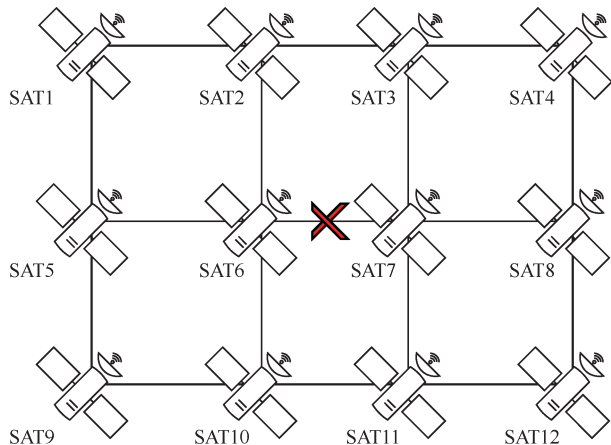


图5 链路故障快速恢复机制示例

3 路由攻击场景仿真及分析

在完成星间路由安全机制设计之后，本文搭建网络仿真平台对其有效性进行验证。根据实现方式的不同，主流卫星网络仿真平台可以分为基于离散事件的仿真^[19]和基于容器与虚拟化技术的仿真^[20]两类。其中，基于容器与虚拟化技术的网络仿真平台基于虚拟网络设备实现流量的

仿真处理，能够承载真实网络流量，复现真实网络设备的数据包处理行为，具有较高的保真度。因此，本文基于容器与虚拟化技术设计并实现卫星网络仿真平台，通过动态配置虚拟网络设备之间的连接通断实现低轨卫星网络动态拓扑的仿真，并在仿真平台上搭载星间路由安全机制。同时，利用 Open vSwitch 虚拟交换机^[21]仿真多种路由攻击场景，验证星间路由协议的抗毁性及链路故障再寻路机制的执行效率和资源开销。

3.1 基于虚拟化技术的卫星网络仿真

仿真系统基于 Linux 操作系统研发，使用网络命名空间（Network Namespace, NetNS）对单颗卫星进行仿真，从而为每颗卫星创建单独的网络协议栈。在 NetNS 内部可以运行独立的收发包处理进程，并对真实数据包进行转发。两个 NetNS 间的虚拟网络链路可以通过 Linux 虚拟网络设备 Veth-pair、Bridge 以及 Open vSwitch 进行仿真。这些虚拟网络设备的一端可以归属于某个 NetNS，与整个内核协议栈相连接，从而提供链路构建、数据包收发以及协议栈处理的功能。图6为基于 Linux 虚拟网络设备的星间链路仿真模型，Veth-pair 的两端分别置于两个卫星节点对应的 NetNS 内部，从而提供两个卫星节点间星间链路通断的仿真及数据包收发的功能。

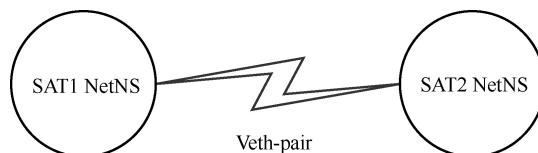


图6 基于 Linux 虚拟网络设备的星间链路仿真模型

通过 NetNS 网络命名空间及虚拟网络设备搭建低轨卫星网络时，需要导入卫星轨道数据。本文使用卫星场景仿真软件 STK^[22]为网络仿真平台的链路通断配置提供真实的星座参数。后续实验以 LEO48 星座作为仿真场景，卫星运动周期为 6 900 s，利用 STK 生成 LEO48 星座轨道模型下的卫星位置数据并以二进制文件格式导入仿真平台，实现对低轨卫星网络的动态拓扑仿真。

3.2 路由攻击场景仿真

在存在恶意节点的情况下，星间链路上传递的数据包可能会被其他节点窃听、截获、篡改或延迟。为了模拟存在恶意节点和多种安全威胁的流量转发场景，可以在 Open vSwitch 虚拟交换机内部建立多个转发端口，并指定端口之间的数据包转发逻辑。图7为一个简化的存在恶意节点的星间链路仿真模型。具体的，在两个卫星节点之间建立一个 Open vSwitch 虚拟交换机，该虚拟交换机内部建立 3 个端口，分别与星间链路两侧的卫星节

点以及链路中段的恶意节点对应。Veth-pair 是一对虚拟网络设备，其中一端置于卫星节点对应的 NetNS 内部，另一端与 Open vSwitch 的一个端口进行绑定。卫星节点 SAT1 和 SAT2 的 Veth-pair 分别与交换机的 P1 和 P2 端口绑定，而恶意节点的 Veth-pair 与 P3 端口绑定。根据不同的攻击场景，设置 Open vSwitch 端口之间的流量转发逻辑，以模拟不同攻击场景下星间链路的通断以及数据包的收发情况。

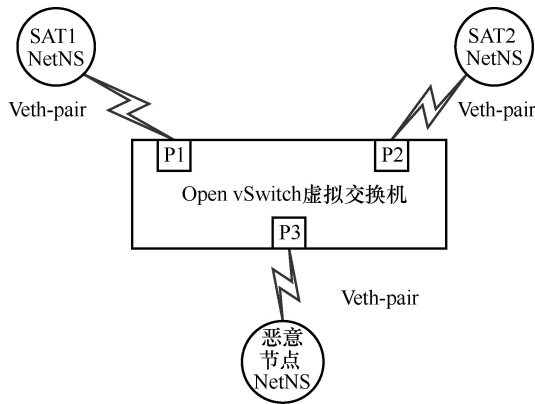


图7 存在恶意节点时的星间链路简化仿真模型

(1) 攻击卫星发送伪造 Hello 报文

卫星节点 SAT1/SAT2 可以通过 P1/P2 端口相互转发报文，以模拟卫星节点之间的报文收发。恶意节点 A 通过与 P3 端口绑定，可以向 P1 和 P2 端口转发报文，从而模拟恶意节点向星间链路注入伪造 Hello 报文的攻击场景。图 8 展示了存在恶意节点发送伪造 Hello 报文时的星间链路仿真模型。

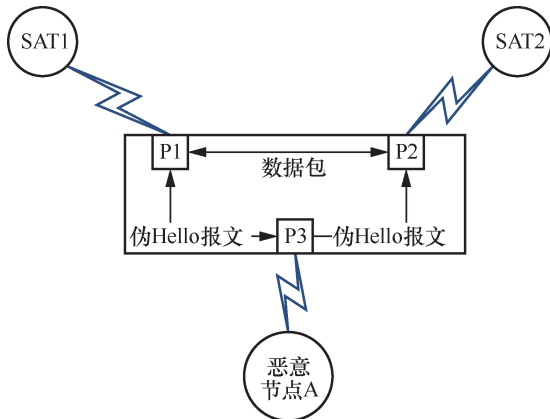


图8 存在恶意节点发送伪造 Hello 报文时的星间链路仿真模型

(2) 攻击卫星截获并丢弃 Hello 报文

卫星节点 SAT1/SAT2 与 P1/P2 端口进行绑定，P1/P2 端口将卫星节点发送的报文转发到 P3 端口，以模拟恶意

节点截获 P1/P2 端口的报文攻击场景。图 9 为存在恶意节点截获并丢弃 Hello 报文时的星间链路仿真模型。

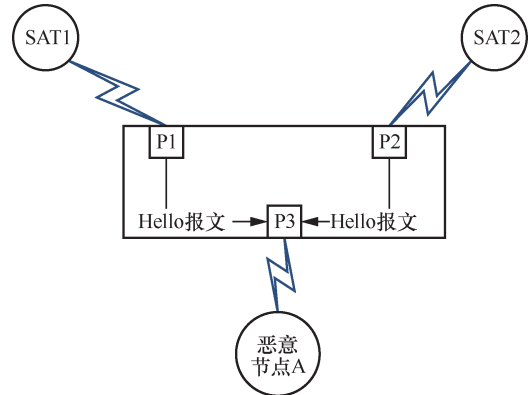


图9 存在恶意节点截获并丢弃 Hello 报文时的星间链路仿真模型

(3) 攻击卫星发送伪造 LSU 报文

卫星节点 SAT1/SAT2 可以通过 P1/P2 端口相互转发报文，以模拟卫星节点之间的报文收发。恶意节点 A 通过与 P3 端口绑定，可以向 P1 端口转发报文，从而模拟恶意节点向星间链路注入伪造 LSU 报文的攻击场景。图 10 为存在恶意节点发送伪造 LSU 报文时的星间链路仿真模型。

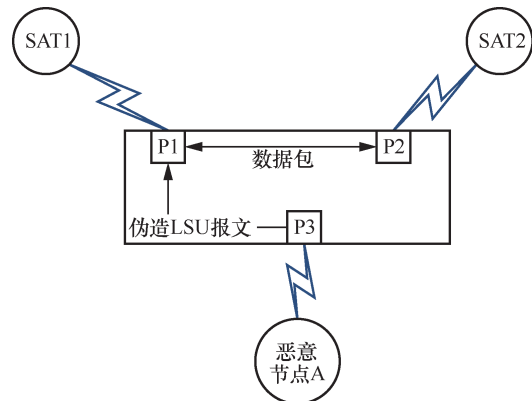


图10 存在恶意节点发送伪造 LSU 报文时的星间链路仿真模型

(4) 攻击卫星截获并篡改 LSU 报文

卫星节点 SAT1/SAT2 可以通过 P1/P2 端口相互转发报文，以模拟卫星节点之间的报文收发。同时，P2 端口将报文转发到 P3 端口，恶意节点 A 通过与 P3 端口绑定来接收来自 SAT2 节点发送的报文，从而模拟恶意节点截获 LSU 报文的场景。P3 端口可以将报文转发到 P1 端口，以模拟恶意节点篡改或延迟 LSU 报文后向卫星网络中注入经过篡改/延迟的报文的攻击场景。图 11 为存在恶意节点截获并篡改/延迟发送 LSU 报文时的星间链路仿真模型。

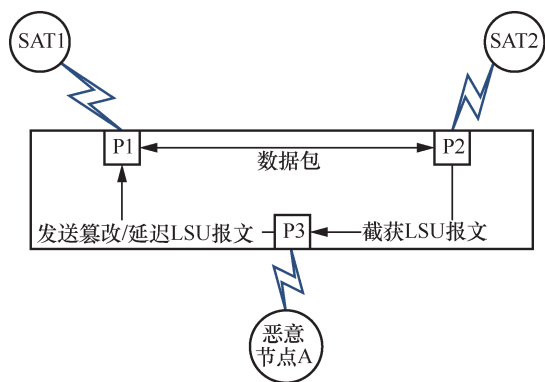


图 11 存在恶意节点截获并篡改/延迟发送 LSU 报文时的星间链路仿真模型

3.3 安全认证机制抗毁性验证

上面提出的星间链路模型，可以仿真针对星间链路的多种路由攻击场景。针对每一种路由攻击场景，可以通过对比加入安全路由认证机制前后发包节点和目的网段的可达性，验证安全认证机制的抗毁性能。

(1) 恶意节点发送伪造 Hello 报文攻击场景

图 12 为恶意节点发送伪造 Hello 报文的 3 种场景（无攻击状态、攻击状态和加入认证机制）的时延对比。在该攻击模式下，恶意节点将持续向星间链路两侧卫星节点发送伪造的 Hello 报文，这些伪造的 Hello 报文将干扰卫星节点对链路状态的感知。本文在 30 s 时断开星间链路以模拟突发链路故障。在未加入安全机制时，两侧卫

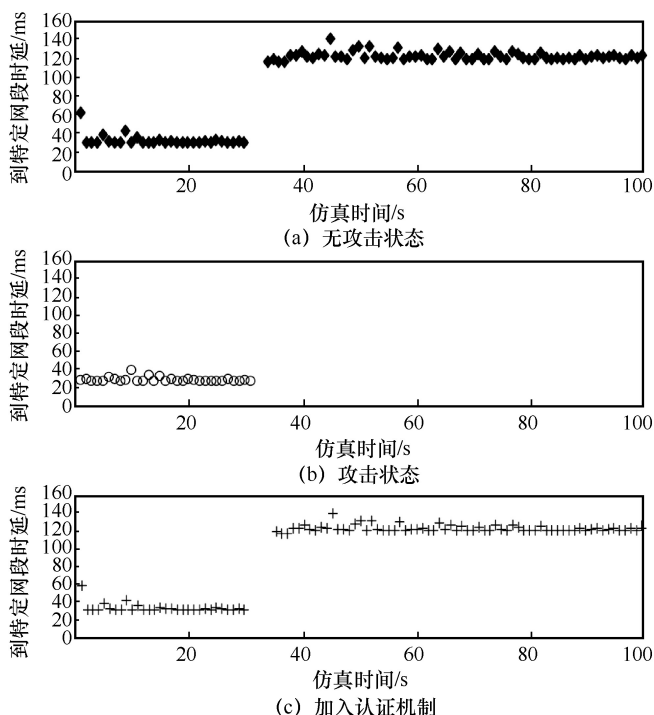


图 12 恶意节点发送伪造 Hello 报文 3 种场景的时延对比

星节点在断开星间链路后将持续收到恶意节点发送的伪造 Hello 报文，无法及时感知真实世界的链路故障，卫星节点不会洪泛 LSU 报文更新链路状态信息及路由表项，仍然向已经断开的星间链路转发数据包，最终导致所有经过该链路的数据包的丢失，造成经过故障链路的通信业务的中断。在加入星间路由安全机制后，卫星节点验证 Hello 报文来源的合法性，将报文鉴别码 HMAC 不匹配的协议包丢弃。星间链路断开时，两侧卫星节点能够及时感知链路故障，从而及时切换路由，快速恢复星间链路通信业务。

(2) 恶意节点发送伪造 LSU 报文攻击场景

图 13 为在恶意节点发送伪造 LSU 报文时，经过受攻击链路的通信业务的时延对比。实验中为了仿真伪造 LSU 报文对空间网络路由安全的影响，令恶意节点在 16 s 时向卫星网络注入一个伪造的 LSU 报文。在未加入安全机制的情况下，当卫星节点接收到伪造的 LSU 报文后，会更新本地的链路状态数据库和路由表，并进行全网洪泛，导致多余的协议包洪泛和路由更新，从而造成通信业务的中断。然而，在加入安全认证机制后，当卫星节点收到来自恶意节点的伪造 LSU 报文时，首先会验证 LSU 报文的鉴别码，如果不匹配，将丢弃伪造的 LSU 报文，并不会进行错误的路由更新，因此通信业务始终不会中断。

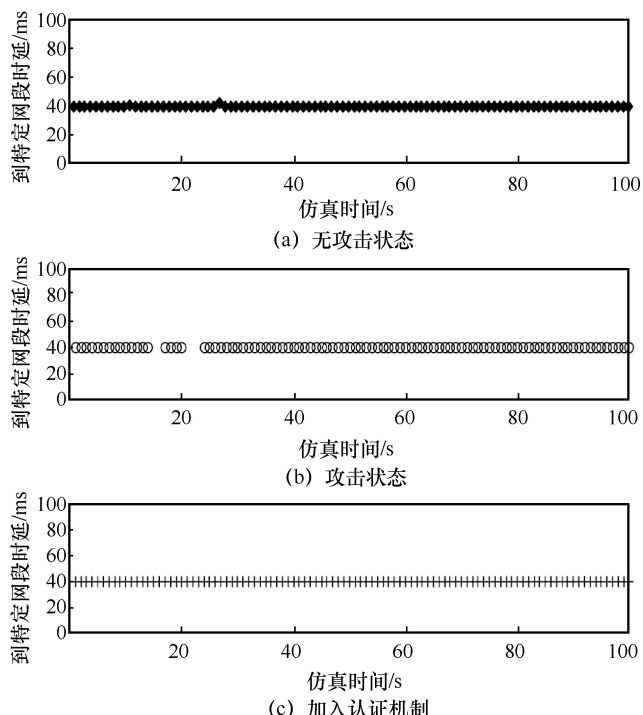


图 13 恶意节点发送伪造 LSU 报文 3 种场景时延对比

(3) 恶意节点截获并篡改 LSU 报文后向卫星网络发送攻击场景

图 14 为 LSU 篡改攻击场景的卫星网络拓扑。在实验中,为了产生 LSU 链路状态更新协议包,30 s 时通过系统命令将 SAT3-SAT4 星间链路断开,路由更新后 SAT1 到 SAT4 间数据包转发路径切换为 SAT1-SAT2-SAT3-SAT11-SAT12-SAT4。70 s 时通过系统命令将所断开的 SAT3-SAT4 星间链路恢复,卫星节点将 LSU 协议包的链路状态信息封装为 SAT3-SAT4 故障链路恢复,并对全网进行洪泛。在路由表再次更新后,SAT1 到 SAT4 间数据包转发路径将切换回 SAT1-SAT2-SAT3-SAT4。此时,恶意节点截获 LSU 协议包并篡改报文信息,将其标记为 SAT3-SAT4 链路故障,并等待一段时间后注入网络。在 90 s 时,恶意节点将篡改过的 LSU 协议包注入卫星网络。在未加入协议包安全认证机制的情况下,当卫星节点接收到篡改后的 LSU 报文时,将重新更新 SAT1 到 SAT4 的数据包转发路径,导致额外的协议包洪泛和路由更新,从而引发通信业务的中断。然而,在星间路由协议引入安全认证机制后,由于篡改后的 LSU 协议包报文鉴别码与卫星节点本地生成的鉴别码不匹配,卫星节点将直接丢弃该协议包,不会进行错误的路由更新,从而保持通信业务的连续性。图 15 为恶意节点篡改 LSU 报文 3 种场景时延对比。

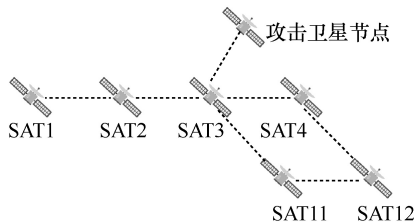


图 14 LSU 篡改攻击场景的卫星网络拓扑

3.4 链路故障再寻路机制性能验证

在星间路由协议中引入快速再寻路机制后,需要验证链路故障再寻路机制的性能。图 16 为在链路故障发生时需要更新的路由条目数量的对比结果。图 17 为在链路故障后更新完所有路由所需的路由收敛时间的对比。实验结果表明,随着星座规模的增加,全局洪泛链路状态信息后需要更新的路由条目逐渐增加,并且更新全部路由达到路由收敛的时间逐渐变长,路由收敛时间受星座规模的影响较大。然而,当使用局部洪泛链路状态信息时,由于洪泛区域始终保持在故障链路周围,需要更新的路由条目数量保持不变,更新全部路由达到路由收敛所需的时间稳定。因此,路由收敛时间不再受星座规模的影响,这实现了对突发链路故障的快速修复,提升了星间网络路由的自愈能力。

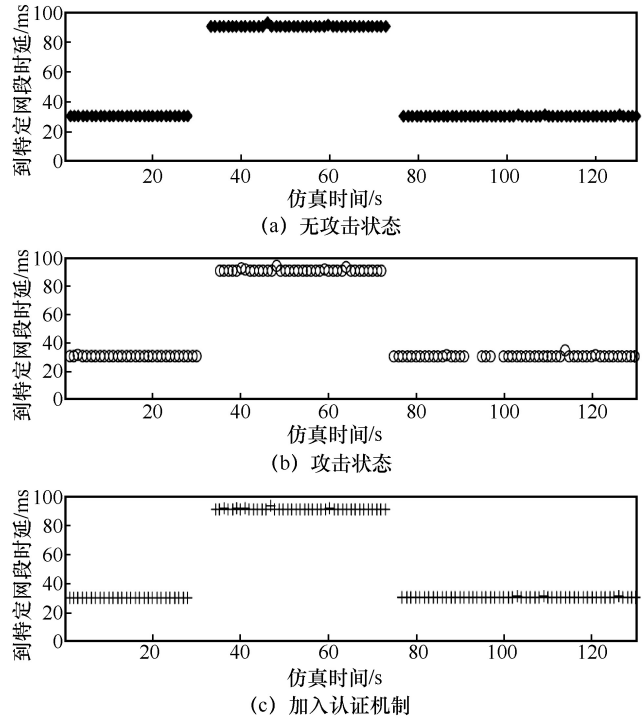


图 15 恶意节点篡改 LSU 报文 3 种场景时延对比

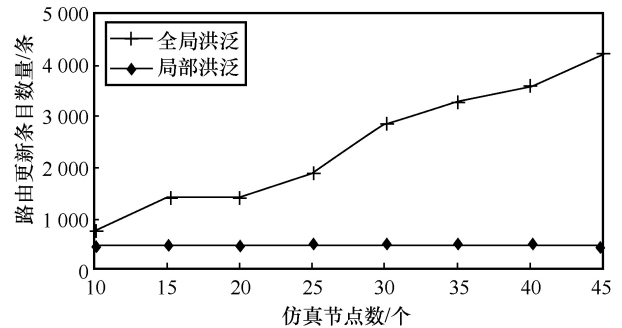


图 16 在链路故障发生时需要更新的路由条目数量的对比

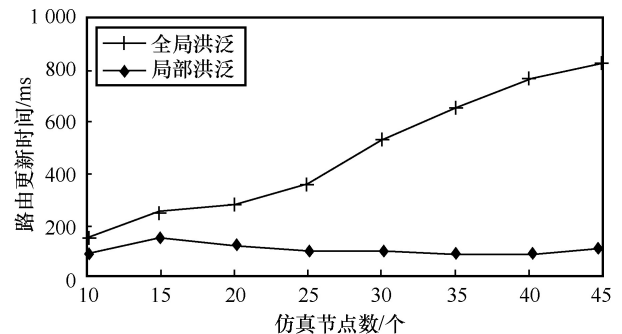


图 17 在链路故障后更新完所有路由所需的路由收敛时间的对比

3.5 路由安全机制额外性能开销

引入安全认证机制后,需要测量执行路由安全认证对系统性能的影响,以避免过多占用星上的存储和计算资

源。图 18 为协议包洪泛时间随星座规模变化的情况。实验结果表明,在加入安全认证机制前后,协议包的总洪泛时间均随着星座规模呈线性增长,而安全机制各个流程所需的时间在协议包总洪泛时间中始终保持较低的占比,且不会随星座规模的变大有明显变化,对协议包的总洪泛时间和路由收敛时间影响较小。由此证明星间路由安全机制能够在有限的认证时间和通信开销下,防范空间网络环境中的多种威胁。

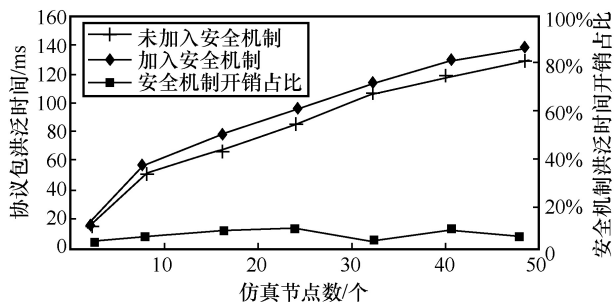


图 18 路由协议包洪泛时间随星座规模变化的情况

图 19 为 0~400 s 内未加入安全机制和加入安全机制后的两种星间路由协议在系统 CPU 利用率方面的对比。对于 LEO48 星座而言,大约每隔 100 s 会发生一次规律性的拓扑通断。在拓扑通断发生时,需要进行快照序列切换和路由表更新,导致 CPU 利用率上升;而在快照序列切换和路由表更新完成后, CPU 利用率将下降。实验结果表明,星间路由协议加入安全机制后, CPU 利用率的变化不明显,执行轻量化的路由安全机制不会对系统性能产生明显影响。

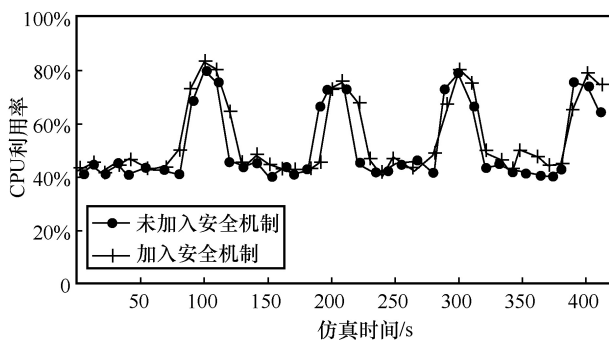


图 19 CPU 利用率对比

4 结束语

后续的工作将进一步设计和完善密钥的分配管理方案以及异常信息的地面通报流程,以实现更加安全高效的星间路由防护。

参考文献:

- [1] MCDOWELL J C. The low earth orbit satellite population and impacts of the SpaceX Starlink constellation[J]. The Astrophysical Journal Letters, 2020, 892(2): L36.
- [2] HENRI Y. The OneWeb satellite system[M]//Handbook of Small Satellites. Cham: Springer International Publishing, 2020: 1-10.
- [3] PAN T, HUANG T, LI X C, et al. OPSPF: orbit prediction shortest path first routing for resilient LEO satellite networks[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2019: 1-6.
- [4] RUAN G H, PAN T, LU C C, et al. Lightweight route flooding via flooding topology pruning for LEO satellite networks[C]//Proceedings of ICC 2022 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 1149-1154.
- [5] 李喆, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006, 27(8): 113-118.
- [6] LI Z, LIU J. Research on secure routing algorithm in satellite networks[J]. Journal on Communications, 2006, 27(8): 113-118.
- [7] ASUQUO P, CRUICKSHANK H, OGAH C P A, et al. A distributed trust management scheme for data forwarding in satellite DTN emergency communications[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(2): 246-256.
- [8] YU Z F, ZHOU H G, WU Z F. A trust-based secure routing protocol for multi-layered satellite networks[C]//Proceedings of 2012 IEEE International Conference on Information Science and Technology. Piscataway: IEEE Press, 2012: 313-317.
- [9] VATALARO F, CORAZZA G E, CAINI C, et al. Analysis of LEO, MEO, and GEO global mobile satellite systems in the presence of interference and fading[J]. IEEE Journal on Selected Areas in Communications, 1995, 13(2): 291-300.
- [10] 孙文宇, 张伟嘉, 王立民. 基于深度不确定性估计网络的低轨卫星互联网故障预测方法[J]. 天地一体化信息网络, 2022(2): 89-97.
- [11] SUN W Y, ZHANG W J, WANG L M. Fault detection method of low-orbit satellite Internet based on deep uncertainty estimation network[J]. Space-Integrated-Ground Information Networks, 2022(2): 89-97.
- [12] 周笛, 盛敏, 郝琪, 等. 巨型星座系统的网络运维与资源管控技术[J]. 天地一体化信息网络, 2020(1): 26-35.
- [13] ZHOU D, SHENG M, HAO Q, et al. Network operation, maintenance and resource management in mega constellation system[J].

Space-Integrated-Ground Information Networks, 2020(1): 26-35.

- [11] 刘沛龙, 陈宏宇, 魏松杰, 等. LEO 卫星网络海量遥感数据下行的负载均衡多径路由算法[J]. 通信学报, 2017, 38(S1): 135-142.
LIU P L, CHEN H Y, WEI S J, et al. Load balancing multipath routing protocol for mass remote sensing data downlink in LEO satellite network[J]. Journal on Communications, 2017, 38(S1): 135-142.
- [12] EKICI E, AKYILDIZ I F, BENDER M D. Datagram routing algorithm for LEO satellite networks[C]//Proceedings of Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064). Piscataway: IEEE Press, 2002: 500-508.
- [13] WERNER M. A dynamic routing concept for ATM-based satellite personal communication networks[J]. IEEE Journal on Selected Areas in Communications, 1997, 15(8): 1636-1648.
- [14] YAN J. Reverse detection based QoS routing algorithm for LEO satellite constellation networks[J]. Tsinghua Science & Technology, 2011, 16(4): 358-363.
- [15] BARRITT B J, EDDY W. SDN enhancements for LEO satellite networks[C]//Proceedings of 34th AIAA International Communications Satellite Systems Conference. Virginia: AIAA, 2016.
- [16] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.
- [17] DOULIGERIS C, SERPANOS D N. Network Security: Current Status and Future Directions[M]. USA: Wiley, 2006.
- [18] MALIK S. Network security principles and practices[Z]. 2002.
- [19] HENDERSON T R, LACAGE M, RILEY G F, et al. Network simulations with the ns-3 simulator[J]. SIGCOMM demonstration, 2008, 14(14): 527.
- [20] LANTZ B, HELLER B, MCKEOWN N. A network in a laptop: rapid prototyping for software-defined networks[C]//Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. New York: ACM, 2010: 1-6.
- [21] PFAFF B, PETTIT J, KOPONEN T, et al. The design and implementation of open vswitch[C]//12th {USENIX} Symposium on Networked Systems Design and Implementation. [S.l.:s.n.], 2015: 117-130.
- [22] QI J Q, LI Z M, LIU G L. Research on coverage and link of multi-layer Satellite Network based on STK[C]//Proceedings of 2015 10th International Conference on Communications and Networking in China (ChinaCom). Piscataway: IEEE Press, 2016: 410-415.

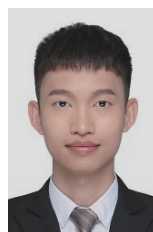
[作者简介]



薛文浩 (1997—), 男, 北京邮电大学硕士生, 主要研究方向为低轨卫星网络、网络安全协议、卫星网络仿真系统等。



潘恬 (1987—), 男, 博士, 北京邮电大学副教授, 博士生导师, 主要研究方向为云数据中心网络、低轨卫星网络、高速可编程网络设备等。



卢诚承 (1998—), 男, 北京邮电大学硕士生, 主要研究方向为低轨卫星网络、分布式路由协议、卫星网络仿真系统等。



杨帆 (1981—), 男, 博士, 北京邮电大学工程师, 硕士生导师, 主要研究方向为软件定义网络、低轨卫星网络、高性能路由交换技术等。



黄韬 (1980—), 男, 博士, 北京邮电大学教授, 博士生导师, 主要研究方向为未来网络体系架构、软件定义网络、确定性网络等。



刘韵洁 (1943—), 男, 中国工程院院士, 主要研究方向为未来网络体系架构、软件定义网络、网络操作系统等。