

电子科技大学
UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA

专业学位硕士学位论文
MASTER THESIS FOR PROFESSIONAL DEGREE



论文题目 LEO 卫星网络的可靠性路由算法研究

专业学位类别 工 程 硕 士

学 号 201822010319

作 者 姓 名 李航

指 导 教 师 廖丹 教授

分类号 _____ 密级 _____

UDC ^{注1} _____

学 位 论 文

LEO 卫星网络的可靠性路由算法研究

(题名和副题名)

李航

(作者姓名)

指导教师	廖丹	教授
	电子科技大学	成 都

(姓名、职称、单位名称)

申请学位级别 硕士 专业学位类别 工 程 硕 士

工程领域名称 电子与通信工程

提交论文日期 2021.5.24 论文答辩日期 2021.5.26

学位授予单位和日期 电子科技大学 2021 年 6 月

答辩委员会主席 蒋定德

评阅人 章小宁、蒋定德

注 1: 注明《国际十进分类法 UDC》的类号。

Research on Reliability Routing Algorithm of LEO Satellite Network

A Master Thesis Submitted to
University of Electronic Science and Technology of China

Discipline: **Master of Engineering**

Author: **Hang Li**

Supervisor: **Dan Liao**

**School of Information and Communication
Engineering**

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名：



日期：2021年 6 月 4 日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

作者签名：



导师签名：



日期：2021年 6 月 4 日

摘要

LEO 卫星通信系统具有通信时延低、研发成本低以及通信组网灵活等优势，受到了各航天科技大国的重点关注。而高效、可靠的星间路由算法对卫星网络性能发挥至关重要。但是，目前的 LEO 卫星网络星间路由算法在可靠性方面仍然存在诸多挑战：一方面，由于 LEO 卫星网络的高动态拓扑变化、全球流量分布不均衡，致使卫星节点和链路易发生拥塞；另一方面，由于受星间链路稳定性差、开放性、暴露性等特点的影响，网络内部路由易遭受恶意攻击。

因此，为了解决以上的问题，本文深入研究了 LEO 卫星网络的可靠性路由算法。具体的研究内容如下：

(1) 针对卫星节点和链路的拥塞问题，提出了基于 QoS 保障的 LEO 卫星网络可靠性路由算法。该算法从 QoS 保障角度考虑，通过减小卫星节点和链路拥塞发生概率，降低因拥塞导致队列溢出所产生的丢包，提高路由转发的可靠性。首先，基于改进的轨道发言人机制完成全网链路状态数据库更新，并构建一种多 QoS 约束且能实现全球流量均衡分布的最优路由模型。其次，采用拓扑剪枝预处理以及拉格朗日松弛技术完成最优路径的求解，若最优路径不存在则计算一条缺省路径。然后，将求得的最优路径或缺省路径采用压缩编码机制转换，得到用以指导数据包实际路由转发的路径 ID 表。最后，经仿真测试验证，此算法在平均端到端时延、丢包率、吞吐量、流量均衡指数以及归一化链路负载等方面均表现不错。

(2) 针对卫星网络中潜在的内部路由攻击问题，提出了一种基于节点信任度的 LEO 卫星网络安全路由算法。该算法从路由安全角度考虑，通过及时检测和隔离卫星网络中恶意节点，降低因恶意节点发动诸如黑洞、灰洞等攻击造成数据包被恶意丢弃的影响，提高路由转发可靠性。首先，利用 D-S 证据理论构建一套用于评估卫星节点信任度的动态信任评估模型，包括直接信任、间接信任以及聚合信任模型的设计。然后，采用此套信任评估模型对一种低开销基于轨道预测的 LEO 卫星网络路由算法进行安全信任加固，设计出基于节点信任度的 LEO 卫星网络安全路由算法，包括基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块的设计。最后，经仿真测试验证，此算法在分组投递率、丢包率均表现不错。

关键词：LEO 卫星网络，可靠路由，QoS，安全

ABSTRACT

The LEO satellite communication system has the advantages of low communication delay, low research and development cost, and flexible communication networking, and has attracted the attention of major aerospace countries. An efficient and reliable inter-satellite routing algorithm is crucial to the performance of satellite networks. However, the current LEO satellite network inter-satellite routing algorithm still has many challenges in terms of reliability: on the one hand, due to the highly dynamic topology changes of the LEO satellite network and the uneven global traffic distribution, the satellite nodes and links are prone to congestion; on the other hand, the satellite nodes and links are prone to congestion; On the one hand, due to the poor stability, openness, and exposure of inter-satellite links, the internal routing of the network is vulnerable to malicious attacks.

Therefore, in order to solve the above problems, this article deeply researches the reliability routing algorithm of LEO satellite network. The specific research content is as follows:

(1) Aiming at the congestion problem of satellite nodes and links, a reliable routing algorithm of LEO satellite network based on QoS guarantee is proposed. From the perspective of QoS guarantee, this algorithm reduces the probability of congestion of satellite nodes and links, reduces packet loss caused by queue overflow due to congestion, and improves the reliability of routing and forwarding. First, complete network-wide link state database update based on the improved track spokesperson mechanism, and build an optimal routing model with multiple QoS constraints and a balanced distribution of global traffic. Second, topological pruning preprocessing and Lagrangian relaxation technology are used to solve the optimal path. If the optimal path does not exist, a default path is calculated. Then, the obtained optimal path or default path is converted using a compression coding mechanism to obtain a path ID table used to guide the actual routing and forwarding of the data packet. Finally, the simulation test verifies that this algorithm performs well in terms of average end-to-end delay, packet loss rate, throughput, traffic balance index, and normalized link load.

(2) Aiming at the potential internal routing attacks in satellite networks, a safe routing algorithm for LEO satellite networks based on node trust is proposed. From the

perspective of routing security, the algorithm can detect and isolate malicious nodes in satellite network in time, reduce the impact of malicious packet discarding caused by malicious nodes launching attacks such as black holes and gray holes, and improve the reliability of routing and forwarding. Firstly, a set of dynamic trust evaluation model is constructed by using D-S evidence theory, including the design of direct trust, indirect trust and aggregate trust model. Then, this set of trust evaluation model is used to strengthen the security trust of a low-overhead LEO satellite network routing algorithm based on orbit prediction, and a secure routing algorithm based on node trust degree is designed, including basic routing modules and dynamic trust evaluation processing Module and design of dynamic health diagnosis processing module. Finally, the simulation test verifies that this algorithm performs well in both packet delivery rate and packet loss rate.

Keywords: LEO satellite network, Reliable routing, QoS, Security

目 录

第一章 绪 论	1
1.1 研究背景及意义	1
1.2 国内外研究现状	3
1.3 本论文主要内容及贡献	6
1.4 本论文结构安排	7
第二章 卫星通信系统及路由技术概述	8
2.1 卫星通信系统分类	8
2.1.1 依据轨道高度划分	8
2.1.2 依据轨道动力学划分	8
2.1.3 依据通信组网方式划分	9
2.2 星座式卫星网络	10
2.2.1 星座式卫星网络种类	10
2.2.2 低轨卫星星座分析	11
2.3 卫星网络路由技术	12
2.3.1 路由域分析	12
2.3.2 路由面临挑战	13
2.4 本章小结	14
第三章 基于 QoS 保障的 LEO 卫星网络可靠性路由算法	15
3.1 引言	15
3.2 基础概念及相关定义	16
3.2.1 卫星星座模型	16
3.2.2 相关参数定义	17
3.3 算法设计	19
3.3.1 基本思想	19
3.3.2 全网链路状态数据库更新	21
3.3.3 可靠性路由模型建立	23
3.3.4 路由模型求解	24
3.3.4.1 存在最优解	24
3.3.4.2 不存在最优解	27
3.3.4.3 路径信息压缩编码	27

3.4 仿真设计及结果分析	29
3.4.1 仿真环境和参数设置	30
3.4.2 仿真结果分析	32
3.5 本章小结	36
第四章 基于节点信任度的 LEO 卫星网络安全路由算法	37
4.1 引言	37
4.2 基于 D-S 证据理论的 LEO 卫星网络信任评估模型	38
4.2.1 D-S 证据理论知识	39
4.2.1.1 基础定义	39
4.2.1.2 Dempster 合成法则	40
4.2.2 卫星网络直接信任模型	40
4.2.3 卫星网络间接信任模型	43
4.2.4 卫星网络聚合信任模型	45
4.3 算法设计	45
4.3.1 基本思想	45
4.3.2 基础路由模块	49
4.3.2.1 位置信息推导阶段	50
4.3.2.2 LSDB 初步建立阶段	52
4.3.2.3 LSDB 修正阶段	53
4.3.2.4 路由计算阶段	53
4.3.2.5 本地端口状态标识更新阶段	54
4.3.3 动态信任评估处理模块	54
4.3.3.1 恶意卫星节点处置	54
4.3.3.2 风险通知 LSU 报文处理	55
4.3.4 动态健康诊断处理模块	56
4.3.4.1 动态检测链路故障发生与处置	57
4.3.4.2 动态检测链路故障恢复与处置	57
4.3.4.3 健康通知 LSU 报文处理	58
4.4 仿真设计及结果分析	59
4.4.1 仿真环境和参数设置	60
4.4.2 仿真结果分析	62
4.5 本章小结	64
第五章 全文总结与展望	65

5.1 全文总结	65
5.2 后续工作展望	66
致 谢	67
参考文献	68
攻读硕士学位期间取得的成果	72

第一章 绪论

1.1 研究背景及意义

由于地球表面还存在着像海洋、荒漠以及山区等环境较为恶劣的通信场景。如果只是采用架设传统地面通信网络的方式，来完成对这些互联网渗透率低的地地区的有效通信覆盖，存在着很大的难度。而且，其建设与运营维护成本也是颇高的。因此，作为地面通信网络的有效延伸与扩展，卫星通信网络凭借其广袤的覆盖范围、可摆脱地理环境限制、组网通信灵活等诸多优点，轻松完成了全球通信的无缝覆盖目标。并且在遥感、导航、军事以及紧急救援等领域充当着愈加重要的角色。因此，本文开展卫星通信网络的研究，对于国家国防建设、商业应用以及满足人民日常通信需求具有重大的战略意义^[1]。

早期对于卫星通信网络的研究，多集中在地球同步轨道（Geostationary Earth Orbit, GEO）卫星系统。仅采用 3 颗 GEO 卫星组网的方式，便可实现对全球中低纬度地区的覆盖^[2]。我国的“天通一号”系统^[3]就是典型的 GEO 卫星通信系统代表之一，能够为地面用户提供卫星电话、电报等对通信质量以及时延要求不高的服务。由于 GEO 卫星距离地面较远，因此，其传播时延与传播损耗性能指标是较高的，不易达到地面用户对于数据传输的实时性与可靠性的要求。而且 GEO 卫星研发周期较长、研发成本较高、服务功能单一。因此，GEO 卫星不符合未来空间信息网的发展趋势，逐渐被各国冷落。而处于中等轨道高度（Medium Earth Orbit, MEO）卫星系统，能够为地面提供导航定位、气象和遥感等服务。其典型代表有 GPS 与 BDS 全球导航卫星系统。但是，MEO 卫星在传播时延与信号衰减等方面的性能表现也不太理想。而幸运的是，处于低轨道高度（Low Earth Orbit, LEO）卫星系统。与前两者相比，其距离地面最近，传播时延与传播损耗性能表现也最佳，并具有支持较高速率数据传输的特长。且其研发与维护成本低、研发周期也短。因此，对于 LEO 卫星通信网络系统的研究，受到了各航天科技大国的广泛关注与重点投入。图 1-1 展示的是 LEO 卫星通信系统各发展阶段的卫星代表系统。

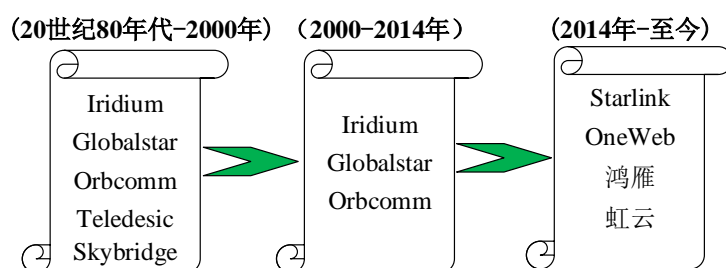


图 1-1 LEO 卫星通信系统各发展阶段卫星代表系统

LEO 卫星通信系统在历经三个阶段的演进后,日渐成熟并被广泛应用。可分为:20 世纪 80 年代~2000 年,与地面通信网络直接展开竞争的第一阶段;2000~2014 年,充当地面通信网络的补充与备用的第二阶段;2014 年~至今,与地面通信网络进行交融发展,扩展市场占有率的第三阶段。在第一发展阶段时,各公司争相推出了各自的 LEO 卫星通信系统。其中,美国摩托罗拉公司于 1987 年开始研发具有 66 颗卫星所组成的 Iridium 星座^[4]系统。美国劳拉与美国高通公司于 1991 年推出了具有 48 颗卫星组成的 Globalstar 卫星通信系统^[5]。美国微软、波音以及麦考等公司于 1994 年联合推出了具有 288 颗卫星组成的 Teledesic 卫星系统^[6]。以及还有美国轨道通信公司推出的 Orbcomm 系统^[7]和由法国阿尔卡特与美国劳拉公司共同筹建的 Skybridge 卫星通信系统^[8]等;在第二发展阶段时,主要是对第一阶段所提出的一些卫星通信系统进行升级换代。在 2006 年时,阿尔卡特·阿列尼亚公司开始着手 Globalstar 系统的升级改造。美国 Lockheed Martin 公司与欧洲 Thales Alenia Space 公司于 2008 年开始竞争完成下一代 Iridium 星座卫星系统的研发升级;进入第三发展阶段时,OneWeb^[9]公司推出了具有 720 颗卫星构成的卫星系统,美国 SpaceX 公司更是欲搭建由 12000 颗卫星构成的 Starlink^[10]卫星通信系统。而我国航天科工集团也相继推出了具有 156 颗卫星构成的“虹云^[11]”和由 270 颗卫星构成的“鸿雁^[12]” LEO 卫星通信系统,分别计划于 2022 年和 2025 年完成组网运营。

由以上介绍可知,针对 LEO 卫星通信系统的研究正迎来前所未有的热潮。所以,本文重点研究 LEO 卫星通信网络下的相关关键技术。作为 LEO 卫星网络关键技术之一的星间路由算法,其效果好坏直接影响了卫星网络性能的发挥。因此,研究适用于 LEO 卫星网络的高效、可靠路由算法至关重要。

处于外太空复杂电磁环境下的 LEO 卫星通信网络:一方面面临由于卫星高速运动所造成的频繁拓扑变化,以及星上资源有限、全球流量分布不均衡、节点与链路易发生拥塞等问题的挑战^[13];另一方面受由于星间链路(Inter-Satellite-Link, ISL)频繁变化所造成的链路稳定性较差,以及 ISL 开放性、暴露性等特点的影响。卫星网络中的正常节点易受到来自恶意节点的干扰、截获等攻击,对空间数据的传输造成了极大的安全威胁。我们国家的“鑫诺号”科教卫星,就曾经在 2003 年,遭到了非法分子的恶意劫持。通过其传播谣言,从事非法活动,对我国社会的和谐与稳定造成了十分恶劣的影响。可见空间网络中的安全问题^[14]也变得日益严峻。

传统地面网络的路由算法由于难以适应 LEO 卫星网络的高动态拓扑变化,因此,不能直接应用于卫星网络这种特殊的网络环境下。故亟需针对 LEO 卫星网络中上述两方面的问题与挑战,设计出具有动态适应性、安全性与可靠性考虑的星间路由算法。实现数据能够在 LEO 卫星网络中,被较为可靠与安全地传输。

1.2 国内外研究现状

近年来,为了解决 LEO 卫星网络的数据传输问题,国内外学者们提出了一些路由解决方案,并取得了一定的成果。本文根据路由设计时侧重点的不同,将 LEO 卫星网络路由算法划分为三大类:经典路由算法、考虑网络资源与业务需求的路由算法、安全路由算法,如图 1-2 所示。

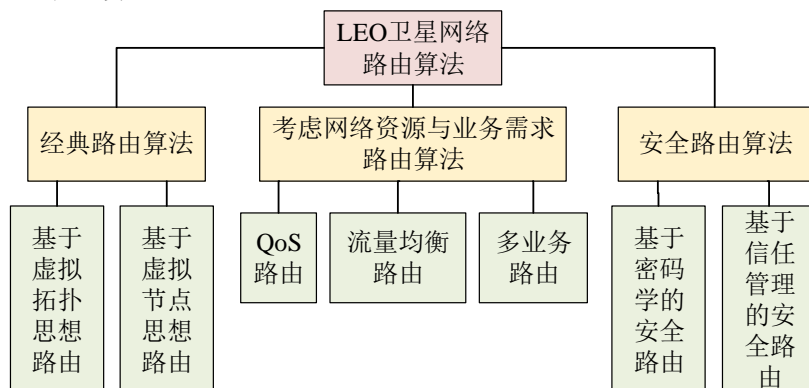


图 1-2 LEO 卫星网络路由算法分类

(1) 经典路由算法

早期经典路由算法以屏蔽卫星高动态运动为设计初衷。从时间虚拟化角度,屏蔽卫星运动,提出了基于虚拟拓扑思想的路由。从空间虚拟化角度,屏蔽卫星高速运动,提出了基于虚拟节点思想的路由。

文献[15]为基于虚拟拓扑思想的路由(Discrete Time Dynamic Virtual Topology Routing, DT-DVTR)。从时间虚拟化角度屏蔽卫星运动。首先利用卫星运动的周期性、规律性特点,将卫星的周期性运动离散化为一系列连续时间间隔划分的固定静态拓扑。然后由地面站在静态拓扑的基础上运行 k -最短路径算法,计算任意两卫星间的临时备用路径集合。并选定相邻两时间片切换最少的路径为最终传输路径,完成离线式路由表的更新,并传至各对应卫星进行存储。接下来,卫星就可依照对应时间片的相应路由表,完成数据的路由转发。但是,DT-DVTR 算法只是选择了最短路径来完成数据的传输。忽略了卫星节点和链路资源的实际占用情况,在网络较为拥塞时,性能表现不佳。

文献[16]是一种基于虚拟节点思想的数据报路由算法。从空间虚拟化角度屏蔽卫星运动。该算法将地球表面等分为若干逻辑区域,并为每个逻辑区域设置一个虚拟节点地址,物理卫星可自动完成与虚拟节点地址的映射与切换,基于虚拟的节点地址完成每个地址到其他地址的路径计算。但是,此路由算法将流量过多地导向高纬度地区,虽然自带一定的拥塞处理机制,但不能从根本上抑制节点拥塞情况的发生。

(2) 考虑网络资源与业务需求的路由算法

根据 LEO 卫星网络所能提供的网络资源以及地面用户的业务需求, 完成此类路由算法的设计。此类路由大致可分为服务质量 (Quality of Service, QoS) 路由、流量均衡路由以及多业务路由。

首先, 对于 QoS 路由的设计。文献[17]提出了一种基于跨层联合和改进蚁群的 LEO 卫星网络多 QoS 约束路由算法。此策略在进行路由选择时, 把物理层的信道情况也进行跨层联合考虑, 并构建了一种多 QoS 约束的最优路由模型, 通过改进的蚁群算法完成路由模型的求解。但是, 此算法并没有考虑引导全球流量的均衡分布, 且通过移动代理的方式完成路径信息的收集, 计算开销较大。

然后, 对于流量均衡路由的设计。文献[18]提出了一种显式流量均衡路由算法 (Explicit Load Balancing, ELB)。此算法中, 卫星会不断监测自身各链路队列占用。并依照链路队列占用信息, 来定义卫星节点的忙碌状态程度。相邻卫星可通过 ISL 显式交换拥塞状态信息。当卫星节点变得十分忙碌时, 它会主动向其上游邻居卫星节点发送通知, 告知其拥塞状态信息。作为回应, 相邻上游卫星会寻找不包含该十分忙碌卫星节点的新路径, 实现流量的分流。虽然 ELB 算法的多路径手段在流量均衡方面具有一定的效果。但是, 其流量均衡范围仅限于局部。因此, 流量均衡能力有限。文献[19]提出了一种基于红、黄、绿信号灯的流量均衡路由算法, 也是一种局部流量均衡路由算法。在该算法中, 首先预规划两条路径, 使得数据包在进行下一跳转发时都有两个选项。然后, 同时考虑卫星节点输出链路队列占用情况与下一跳卫星节点的拥塞情况, 把每条链路采用红、黄、绿三种不同的信号灯颜色进行表示。最后, 卫星节点根据信号灯的颜色, 动态选择一条负载较轻的路径完成数据转发, 具有较优的时延与吞吐性能。但是, 此算法不是从全局视图角度来实现流量均衡, 因此, 很难在全网范围内有效消除流量拥塞。文献[20]提出了一种基于拥塞预测的流量均衡路由算法 (A load balanced routing algorithm based on congestion prediction for LEO satellite networks, LBRA-CP), 以实现在整个 LEO 卫星网络范围内的有效流量均衡。首先, 建立了一个多目标优化模型, 该模型不仅采用修正因子来调整路径代价。而且还采用了拥塞预测的方式, 来预测星间链路拥塞。然后, 利用改进蚁群算法对该模型进行求解, 为每个连接请求找到一条最优路径。但是, LBRA-CP 采用的是基于移动代理的方式, 来完成对全网路径信息的收集, 计算开销颇高。

最后, 对于多业务路由的设计。文献[21]提出了一种多业务按需路由算法。此算法根据 LEO 卫星网络拓扑结构的确定性, 进行路由请求域的限制, 在限制请求域内完成路由请求和路由回复。为不同业务类型的数据寻找各自的最优路径, 但

求得的是局部最优解。且因为是按需路由，故初期等待时延较长。文献[22]提出了一种基于模糊逻辑的路由算法（Fuzzy Satellite Routing Strategy, FSRS）。通过模糊逻辑运算求得每颗卫星拥塞程度。同时，对不同 QoS 要求的数据包区别对待，以满足多类服务质量需求。但是，FSRS 运算复杂度过高。所以，对计算资源有限的 LEO 卫星造成了较为沉重的负担。

（3）安全路由算法

LEO 卫星网络的安全路由算法可分为基于密码学的方案与基于信任管理的方案。前者用于处理网络外部恶意攻击行为，后者用于处理网络内部恶意攻击行为。

基于密码学的安全路由算法。大致可分为基于证书的密码学方案、基于私钥的密码学方案以及基于身份的密码学方案。基于证书的密码学方案^[23]，虽然在地面 ad hoc 网络中已经较为完善与成熟。但是，将其直接适应在卫星网络上却不太合适，因为卫星拓扑结构具有频繁变化的特点，导致卫星节点被截获可能性较大，密钥可能被泄露，最终导致节点被内部攻击。基于私钥的密码学方案^[24]，虽然加密速度较快。但是，此方案不能确保不可否认性，若密钥被攻击者截获，攻击者就可以轻松解密。而且，卫星网络中的节点需要共享长期密钥。然而，卫星是高动态运动的。因此，对于卫星网络中的长期密钥动态生成与管理是极为困难的。文献[25]基于身份的密码学方案，提出了一种 LEO 卫星网络的安全按需路由算法（Secure On-demand Routing, SOR）。SOR 算法同样在受限路由请求域^[21]内，完成路由请求与路由回复。并且对路由控制信息实施签密，在攻击发生前建立防护措施，有效处理网络外部攻击所造成的各种路由安全威胁。然而，由于集中式权限的缺失，网络的服务可靠性会受到数据包转发过程中理性节点自私行为的严重影响。文献[26]提出了一种基于软件定义网络技术的 LEO 卫星网络安全可靠路由算法（A Safe and Reliable Routing Mechanism of LEO Satellite Based on SDN, SRRM）。为了提高卫星网络的可靠性，SRRM 算法首先引入了 SDN 技术。然后，基于曲线参数传输模糊加密算法，设计了一种安全可靠的状态评估决策路由机制，确保了数据在 LEO 卫星网络中能够被安全、有效传输。

基于信任管理的安全路由算法。文献[27]提出了一种基于节点信誉度的安全路由算法。此算法首先采用静态配置与动态调整相结合的策略，能够实现在网络拓扑发生变化时及时作出路由调整。同时，通过节点间的相互协作来维护每个节点的多维信任值以评估节点的行为，及时检测出恶意行为节点，并迅速做出后续安全处理。文献[28]提出了一种基于网络状态和信誉自适应的安全路由算法（Network Status and Reputation Adaptive QoS Dynamic Routing for Satellite Networks, SRADR）。SRADR 算法以网络状态和卫星节点的信誉值为依据，利用蚁群优化算

法进行路由发现和动态更新维护。选择综合性能和安全性能皆优的路径，完成数据的可靠路由转发。文献[29]也是一种基于信任管理的安全路由算法。首先，提出了一种基于滑动窗口机制的卫星网络信任评估模型，然后，采用此信任评估模型，对一种已有卫星网络路由算法实施安全信任加固。采用信任度约束进行路径选择，并以流量均衡为最优化目标。最终，可得到适用于卫星网络的按需安全路由算法。可较好防范常见内部攻击行为。

1.3 本论文主要内容及贡献

为实现 LEO 卫星网络下的可靠性路由算法设计，本文从 QoS 保障和路由安全为切入点，分别针对卫星节点和链路的拥塞问题以及卫星网络中潜在的内部路由攻击问题，设计了各自的可行解决方案。具体的研究内容以及贡献点如下所示：

(1) 针对卫星节点和链路拥塞问题，提出了基于 QoS 保障的 LEO 卫星网络可靠性路由算法。首先，基于改进的轨道发言人机制完成全网链路状态数据库更新。其次，构建一种多 QoS 约束且能够实现全球流量均衡分布的最优路由模型。此模型能够实现在保障路径 QoS 前提下，尽量引导全球流量均衡分布。减小拥塞发生概率，降低因拥塞导致队列溢出所产生的丢包，提高路由转发的可靠性。接下来，接连采用拓扑剪枝预处理以及拉格朗日松弛技术完成最优路由模型求解，若最优路径不存在则计算一条缺省路径。然后，由于此算法采用的是源路由策略，因此，为降低存储与控制开销，将求得的最优路径或缺省路径采用压缩编码机制，转换成用以指导数据包实际路由转发的路径 ID 表。最后，通过仿真验证，此算法在平均端到端时延、丢包率、吞吐量、流量均衡指数以及归一化链路负载等方面均有不错的表现。

(2) 针对卫星网络中潜在的内部路由攻击问题，提出了基于节点信任度的 LEO 卫星网络安全路由算法。首先，基于 D-S 证据理论设计一套用于评估 LEO 卫星网络节点信任度的动态信任评估模型。此模型不需要任何集中式或分布式可信基础措施，通过卫星节点的分布式协作便可实现节点信任度的更新。包括直接信任、间接信任以及聚合信任模型的设计。然后，采用此套信任评估模型对一种基于轨道预测的低开销 LEO 卫星网络路由算法，进行安全信任加固改造，设计出 LEO 卫星网络的安全路由算法。通过及时检测和隔离网络中恶意卫星节点，降低因恶意卫星节点发起诸如黑洞、灰洞等攻击所造成数据包被恶意丢弃的影响。提高路由转发可靠性，实现数据的安全、可靠传输。包括基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块的设计。最后，通过仿真完成安全性能验证，此算法在分组投递率、丢包率均有不错的表现。

1.4 本论文结构安排

本论文总共有五章，各章节内容结构安排如下：

第一章，主要介绍了本论文的研究背景与意义，以及 LEO 卫星网络路由算法的国内外研究现状。同时，提出本论文主要工作内容与贡献点。

第二章，主要对卫星通信系统及路由相关技术进行阐述。首先，依据轨道高度、轨道动力学以及通信组网方式三种不同的分类方式，对卫星通信系统进行划分。然后，对常用低轨星座式卫星系统进行参数对比，选定本文路由设计过程中所实际使用的星座类型。最后，对卫星系统各路由域以及路由设计所面临的挑战进行简要阐述。

第三章，研究了基于 QoS 保障的 LEO 卫星网络可靠性路由算法。首先，对算法的适用卫星星座以及相关参数进行定义说明。其次，基于改进轨道发言人机制，完成全网链路状态数据库更新。接下来，基于路径 QoS 以及地面用户分布不均匀因素考虑，完成可靠性路由模型建立。然后，采用拓扑剪枝预处理以及拉格朗日松弛技术，完成最优路径求解。最后，仿真验证所提算法，能够从全局优化角度有效解决节点和链路拥塞问题。

第四章，研究了基于节点信任度的 LEO 卫星网络安全路由算法。首先，基于 D-S 证据理论完成 LEO 卫星网络信任评估模型设计，包括直接信任、间接信任以及聚合信任模型的设计。然后，采用此套信任评估模型完成对一种基于轨道预测的 LEO 卫星网络路由算法的安全信任加固。设计出 LEO 卫星网络安全路由算法，包括基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块的设计。最后，仿真验证所提算法，此算法能够有效解决卫星网络中内部路由攻击问题。

第五章，对全文研究内容总结，并对不足之处作后续工作展望。

第二章 卫星通信系统及路由技术概述

本章主要对卫星通信系统及路由相关技术进行阐述。首先，依据轨道高度、轨道动力学以及通信组网方式三种不同的分类方式，对卫星通信系统进行划分。然后，对各类星座式卫星通信系统进行参数对比，并选定实际路由算法设计过程中所使用的星座类型。最后，对卫星通信系统的各路由域，以及路由设计所面临的一些挑战，进行简要阐述分析。

2.1 卫星通信系统分类

2.1.1 依据轨道高度划分

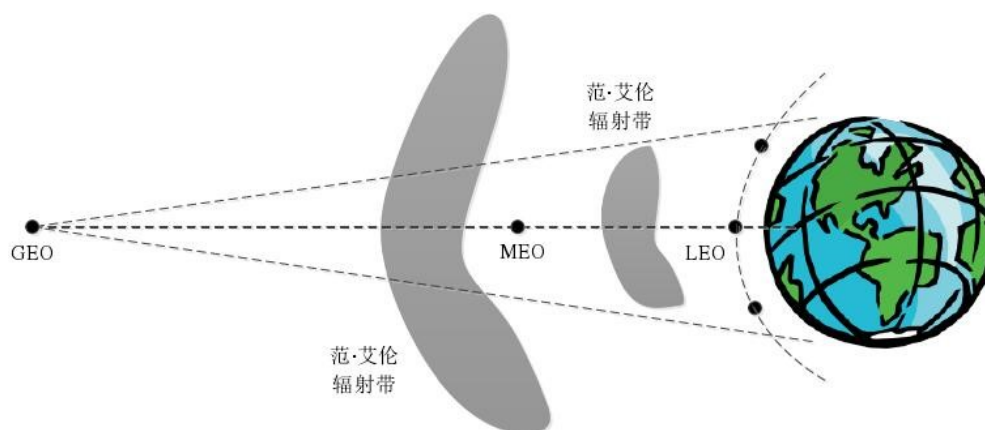


图 2-1 高、中、低轨道高度卫星分布示意图

依据卫星轨道高度，对卫星通信系统进行划分，如表 2-1 所示：

表 2-1 高、中、低轨道高度卫星参数

名称	轨道高度 (km)	运行周期 (h)
GEO 卫星	35786	24
MEO 卫星	5000~20000	2~12
LEO 卫星	500~2000	1.5

2.1.2 依据轨道动力学划分

依据轨道动力学，可将卫星通信系统分为：

(1) 编队飞行。需要对卫星运行轨道和 ISL 外加控制，使得卫星在执行任务过程中能够保持恒定队形。编队内小卫星可执行单项或多项任务，多颗小卫星协

同工作便可媲美大卫星，解决了大卫星功能单一性问题，且具有最佳的抗毁与服务优势。其中，以美国的 F6 计划为典型代表。

(2) 星群。无需对卫星运行轨道和 ISL 外加控制，且由卫星轨道偏离所造成的卫星拓扑变化也无需考虑。通常是由多颗同轨道或异轨道卫星所构成，完成地面监测、空间环境监测等任务。其中，以我国的“吉林一号”分布式星群为典型代表。

(3) 星座。即基于特定分布规则与运行规则的多颗卫星集合。此类构型卫星系统运行于规定轨道之上。如果在运行过程当中，产生了轨道偏差，仅需要通过轨道稍作调整即可。不用再附加其他控制手段，来严格保障卫星网络拓扑。其中，以常见的极轨道星座与倾斜轨道星座为典型代表。

2.1.3 依据通信组网方式划分

依据通信组网方式划分，可将卫星通信系统分为：

(1) 无星间通信链路卫星系统。系统中不具有星间链路，通过弯管的形式进行连接，如图 2-2 所示。

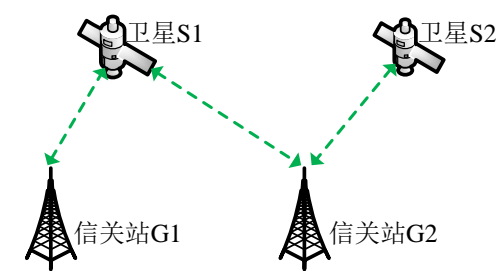


图 2-2 无星间通信链路卫星系统

(2) 有星间通信链路卫星系统。系统中的卫星间通过无线通信链路进行连接，实现卫星间的双向通信，如图 2-3 所示。

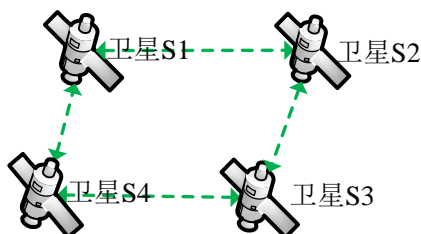


图 2-3 有星间通信链路卫星系统

由以上分类方式可知：由于 GEO 卫星具有距离地面最远、传播时延大、信号衰弱严重以及无法实现对两极地区覆盖的劣势。而 MEO 卫星的运行高度介于 GEO 卫星与 LEO 卫星之间，其传播时延也较高、信号衰减也较为严重。相比于前两者

处于低轨道的 LEO 卫星通信系统具有通信时延小、信号衰减弱以及发射与维护成本低的优势；与编队飞行以及星群式卫星网络构型相比，星座式卫星通信系统具有覆盖范围广、协同能力强的优势；与无星间通信链路、采用弯管式中继转发方式的卫星通信系统相比，具有星间通信链路的卫星通信系统具有数据包转发方便、可实现优化路由设计的优势。

因此，综合以上多种优势的考虑，低轨道且具有星间链路的星座式卫星网络系统是较为理想的卫星通信系统初步选择。

2.2 星座式卫星网络

2.2.1 星座式卫星网络种类

低轨道星座式卫星网络系统常用类型为 2 种：

(1) 极轨道星座。主要通过采用覆盖带的设计方案，由多条倾角约为 90° 的轨道构成。此星座中的所有卫星均匀地分布在各轨道面上，且每个轨道面上卫星数量相同。具有在极地区域分布较为稠密，在赤道区域分布则较为稀疏的特点。且在同一轨道内的相邻卫星间的 ISL 是永久的，而除在极地区域内、反向缝位置时异轨道间 ISL 关闭，其他异轨道间 ISL 是正常建立的，如图 2-4 所示。极轨道星座通常采用一个四元数 $\langle T/M:h:a \rangle$ 来进行完整表示，具体释义如表 2-2 所示。典型代表有 Iridium 星座、LEO48 星座。

表 2-2 四元数 $\langle T/M:h:a \rangle$ 释义

T	M	h	a
星座中容纳卫星总数	轨道面数	轨道高度	轨道倾角

图 2-4 极轨道星座

(2) 倾斜轨道星座。主要通过采用纯几何的设计方案，由多条倾角约为 50° 左右的轨道构成，且要求相邻轨道面间的相位差必须一样。但是，在倾斜轨道星座中维持恒定的 ISL 花费代价颇高，如图 2-5 所示。倾斜轨道星座通常采用一个五元数 $\langle T/M/F:h:a \rangle$ 来进行完整表示，具体释义如表 2-3 所示。典型代表有 Globalstar 星座、GPS 星座。

表 2-3 五元数 $\langle T/M/F:h:a \rangle$ 释义

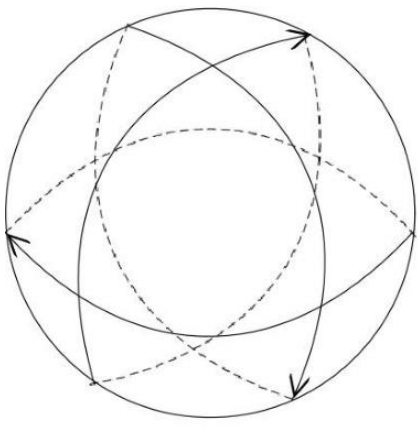
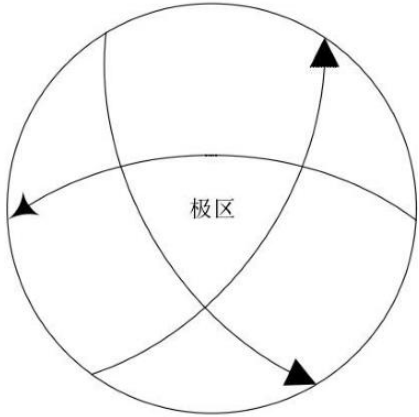
<i>T</i>	<i>M</i>	<i>F</i>	<i>h</i>	<i>a</i>
星座中容纳卫星总数	轨道面数	相位因子	轨道高度	轨道倾角
<div><div><div>N</div><div>S</div></div><div><div>极区</div></div></div>				

图 2-5 倾斜轨道星座

2.2.2 低轨卫星星座分析

表 2-4 常用 LEO 星座参数对比

参数	Iridium	LEO48	Globalstar
高度 (km)	780	1450	1414
卫星总数(颗)	66+6(备份)	48	48+4 (备份)
轨道面数	6	6	8
轨道倾角	86.4°	86°	52°
相位因子	3	3	1
轨道经度差	31.6°	32.6°	45°
极区阈值	70°	70°	90°
周期 (min)	100.13	114.9	113.53
星间链路(条)	2 或 3 或 4	2 或 3 或 4	0

由表 2-4 所示的常用低轨星座各类参数对比可知。属于倾斜轨道星座的 Globalstar 星座，由于 ISL 建立代价较大，所以在 Globalstar 星座中并不具有 ISL，而且 Globalstar 星座系统采用“弯管式”透明转发，卫星仅具有通信中继作用，无 ISL 和星上计算处理能力^[5]。因此，无路由算法设计必要。但是，属于极轨道星座类型的 Iridium 星座^[4]与 LEO48 星座^[30]，不但具有 ISL，且都具有较强的星上计算处理能力，为星间路由算法的运行提供了前提保障。因此，最终决定采用 Iridium 星座作为基于 QoS 保障的 LEO 卫星网络可靠性路由算法的设计场景，采用 LEO48 星座作为基于节点信任度的 LEO 卫星网络安全路由算法的设计场景。

2.3 卫星网络路由技术

2.3.1 路由域分析

早期卫星通信通常是以 3 颗 GEO 卫星作为通信中继，实现“弯管式”的透明数据转发，此类数据转发方式无路由技术可言。但是，在由多颗协同工作的 LEO 卫星，按照一定分布规则所构建的 LEO 星座式卫星通信系统中，每颗 LEO 卫星的星上任务计算处理表现都不错。因此，星上路由算法需要根据给定的链路代价度量，来计算源-目卫星节点对之间的最优路由转发路径。

根据路由域场景的不同，通常将 LEO 卫星通信系统的路由域划分为 3 部分，包括：接入路由域部分、边界路由域部分以及星间路由域部分。各部分路由的地理分布示意，如图 2-6 所示。

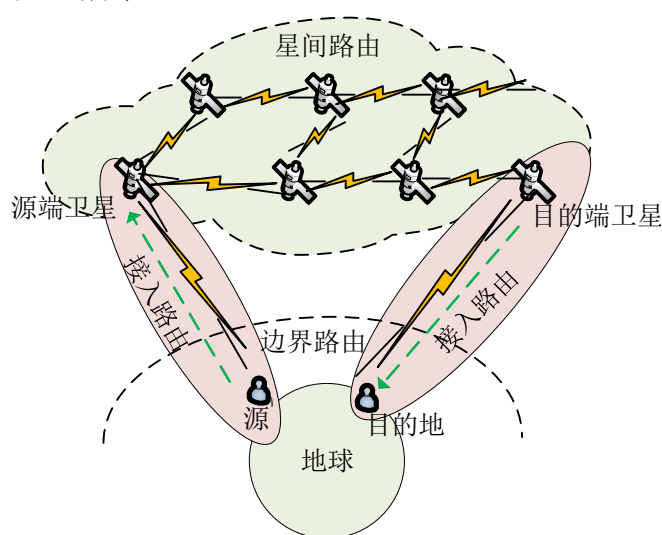


图 2-6 LEO 卫星通信系统各路由域分布示意图

由于，各部分路由所解决问题和承担的任务各不相同，都有各自的侧重点。因此，将各部分路由所实现的功能进行简要介绍，如图 2-7 所示。

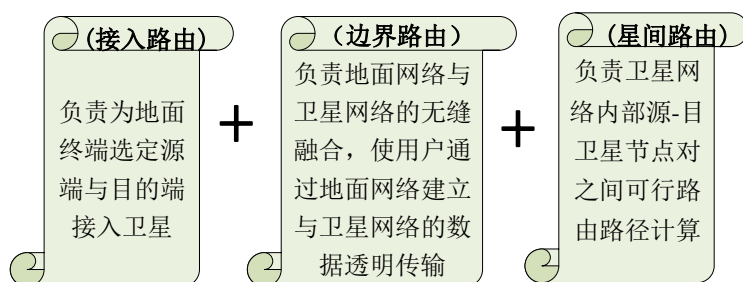


图 2-7 各路由域功能示意图

随着地面用户对于卫星通信服务需求的迅猛增长，以及星上处理能力的日益增强，针对拥有 ISL 的 LEO 卫星网络星间路由算法的设计，具有更加深远的研究前景与收益。国内外研究学者对于 LEO 卫星网络路由算法的研究^[15-29]，也大多集中于星间路由域。星间路由能够摆脱地面控制站繁琐控制，摒弃传统“弯管式”数据中继转发。转而通过多卫星间的相互协作，直接在卫星间完成数据的逐跳转发，为地面终端数据的远程传递，提供一种更为简便高效的路由转发方式。因此，本文路由算法重点研究位于星间路由域的可行路由。

同时，为实现数据的可靠星间路由转发，本文考虑从两个角度设计路由算法，来保障数据传输的可靠性：一种是从路由 QoS 角度考虑，设计了基于 QoS 保障的 LEO 卫星网络可靠性路由算法；另一种是从路由安全角度考虑，设计了基于节点信任度的 LEO 卫星网络安全路由算法。

2.3.2 路由面临挑战

有异于传统地面网络中路由算法的设计考虑。在 LEO 卫星通信网络中，完成可行、高效星间路由算法的设计，面临着如下几点挑战：

（1）卫星网络拓扑呈高动态变化性。星座中的卫星在做绕地高速运动，ISL 的长度以及连接状态在不断变化，如在极圈内、反向缝位置时异轨道间 ISL 难以建立。同时，卫星设备发生故障时也会引起拓扑结构的变化，对于全网链路状态的收集会给星间路由算法的运行带来较大开销。

（2）卫星节点资源受限。由于卫星节点处于遥远复杂的外太空环境中，对于星上设备的升级、换代较为困难，星上计算与存储能力是有限的。因此，需要针对有限的星上资源设计合理的星间路由算法。

（3）传播时延长、误码率高。由于源-目卫星节点对之间的距离远大于地面普通源-目节点对之间的距离，导致传播时延性能指标较差。同时，由于 ISL 易遭受外太空中电磁、噪声干扰等因素的影响，导致误码率性能指标较差。

（4）全球流量分布不均匀。由于受地貌、经济发展等因素的影响，导致地面

用户分布不均匀，存在着流量的热点区域与非热点区域。处于热点区域上空的卫星承担着较大的流量负载压力，而处于非热点上空的卫星则处于较为空闲的状态。如何实现全球流量的均衡分布传输也是星间路由算法所要面临的一大挑战。

(5) 安全威胁。卫星网络中的各卫星节点，是处在复杂的外太空环境当中运行的。因此，受由于 ISL 频繁变化所造成的 ISL 稳定性较差，以及 ISL 开放性、暴露性等特点的影响。极易遭受来自恶意节点的干扰与攻击，对数据的传输造成了极大的潜在安全威胁与挑战。如何抵制和有效处理恶意攻击行为，也应是星间路由算法设计时，所应重点关注与考虑的。

2.4 本章小结

本章首先依据轨道高度、轨道动力学以及通信组网方式三种不同的分类方式，对卫星通信系统进行划分，综合多种优势考虑，初步选定低轨道且具有星间链路的星座式卫星系统。然后，展开对常用低轨道星座式卫星系统的参数对比，选定 Iridium 星座作为基于 QoS 保障的 LEO 卫星网络可靠性路由算法的设计场景，选定 LEO48 星座作为基于节点信任度的 LEO 卫星网络安全路由算法的设计场景。最后，对 LEO 卫星通信系统的各路由域展开介绍，分为接入路由、边界路由以及星间路由三大部分。选定星间路由域，作为本文可靠性星间路由算法的设计重点。同时，也介绍了星间路由设计过程中所可能面临的一些挑战。

第三章 基于 QoS 保障的 LEO 卫星网络可靠性路由算法

3.1 引言

随着空间信息技术的迅猛发展,以及地面用户对于卫星通信服务需求的日益陡增。LEO 卫星通信系统凭借其通信时延低、研发成本低以及通信组网灵活等优势,受到了各航天科技大国的重点关注。而高效、可靠的星间路由算法对卫星网络性能发挥至关重要^[31]。可是,由于 LEO 卫星网络系统所处的外太空环境较为恶劣,且较为复杂,存在着诸如像卫星网络拓扑频繁动态变化、电磁干扰、星上负载不均衡、卫星节点和链路易发生拥塞等情况的发生。因此,为保证提供给地面用户高效、可靠的基础通信服务,使其获得较佳的通信体验感。所以,必须选择一条 QoS 较优且流量负载较轻的路由转发路径,来完成源-目卫星节点对之间数据包的高效、可靠传输。

在本章中,在综合考虑路径 QoS 以及地面用户分布不均匀等因素后,提出了一种基于 QoS 保障的 LEO 卫星网络可靠性路由算法(Reliability routing algorithm of LEO satellite network based on QoS guarantee, RLQ),用以完成源-目卫星节点对之间路由转发路径的搜寻。保证找到的路径具有较优的服务质量,且能够主动实现全球流量的均衡分布。减小卫星发生拥塞的概率,降低因拥塞导致队列溢出所产生的丢包,提高路由转发的可靠性。

本章的主要贡献如下:

(1) 采用改进的轨道发言人机制完成对全网链路状态数据库的更新建立,为路由表的周期性更新做好前提准备。

(2) 对于可靠性路由模型的建立。一方面,为实现路由转发路径具有较佳的服务质量。因此,将时延、带宽等因素考虑进来,进行严格的多 QoS 约束条件限制;另一方面,鉴于全球流量分布不均衡。因此,将卫星节点的地理位置因素考虑进来,定义了一种链路代价修正因子(Location Correction Factor, LCF)。并将 LCF 与链路时延代价相融合,构造成多 QoS 约束优化模型的最优目标函数。引导热点区域流量主动向非热点区域转移分散,实现流量均衡分布。

(3) 对于路由模型的求解。首先,采用拓扑剪枝预处理手段,对多 QoS 约束最优路由模型进行求解降维。然后,基于拉格朗日松弛技术完成最优路径求解,如果最优路径不存在,则计算一条缺省路径。最后,采用压缩编码机制^[32]将求得最优路径或缺省路径转换为路径 ID 表,用以指导数据包的 actual 路由转发,降低存储与控制开销。

3.2 基础概念及相关定义

本节首先对 RLQ 路由算法的适用场景 Iridium 星座进行介绍。然后，对路由设计过程中所使用的相关参数，如链路时延代价、链路可用带宽、链路代价修正因子以及链路状态信息报告进行定义。

3.2.1 卫星星座模型

RLQ 路由算法实验场景为 Iridium 星座，该星座具有 6×11 颗卫星，如图 3-1 所示。若卫星星座中共有 $M \times N$ 颗卫星，则 M 代表的是轨道面数， N 代表的是单个轨道面上的卫星数。为简化由卫星周期性运动导致拓扑高动态变化带来的路由编址难题，因此，引入了逻辑地址概念来标定每个卫星的路由转发地址，逻辑地址记为 $S(m, n)$ 。其中， m 表示第 m 个轨道面， n 表示在第 m 个轨道面上的第 n 颗卫星。且 $0 < m \leq M$ ， $0 < n \leq N$ ， m 与 n 都为正整数。基于逻辑地址的设计理念，在卫星每次进行周期性链路状态信息更新后，可将此时的卫星网络拓扑看成一张由逻辑地址来标定卫星节点地址的静态逻辑平面，方便后续路由算法的设计。

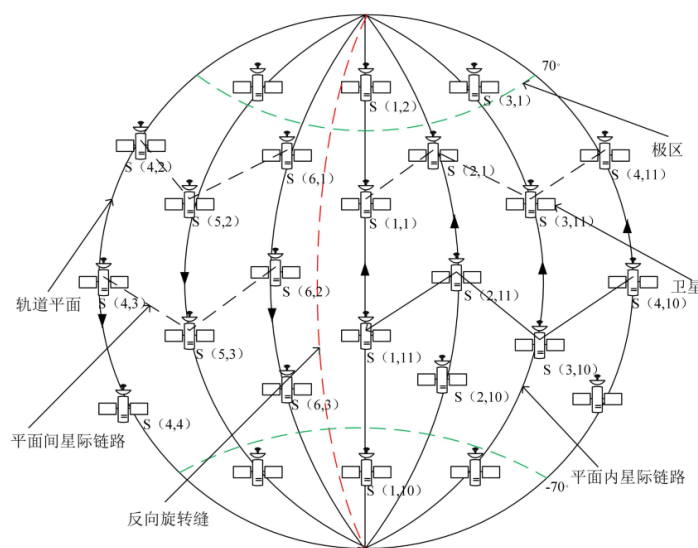


图 3-1 Iridium 星座模型

Iridium 星座中的星间链路 ISL 包括：轨内 ISL 和轨间 ISL。正常情况下，每颗卫星具有 4 条 ISL，即 2 条轨内 ISL 以及 2 条轨间 ISL。但是，也存在两种特殊情况。其一是位于极地区域（即纬度超过 70 度区域）内，由于卫星的高速运动，天线系统难以实时跟踪卫星位置，且极地区域内的用户通信链接需求也极少。因此，异轨间 ISL 会断开。故处于极地区域内的卫星，只具有 2 条轨内 ISL；其二是位于反向缝两侧并作相反运动的卫星。处于反向缝位置时的两颗卫星间的轨间 ISL 并不建立。所以，此位置的卫星只具有 3 条 ISL。

同时需要说明, 轨内 ISL 长度 $Dist_{intra}$ 是一定的, 其连接也是较稳定的。如公式(3-1)所示。其中, N 代表的是单轨道面上卫星数, R_e 代表的是地球半径。

$$Dist_{intra} = \sqrt{2}R_e \sqrt{1 - \cos(\frac{2\pi}{N})} \quad (3-1)$$

而轨间 ISL 长度 $Dist_{inter}$ 是随纬度的增加而减少变化的, 如公式(3-2)所示。其中, M 代表的是轨道面数, lat 代表的是轨道间两相邻卫星间的纬度差。

$$Dist_{inter} = \sqrt{2}R_e \sqrt{1 - \cos(2\pi \frac{1}{2M})} \cos(lat) \quad (3-2)$$

3.2.2 相关参数定义

此部分主要对 RLQ 路由算法设计过程中所使用的星间链路相关参数, 进行定义说明。同时, 本章路由更新采用的是周期性间隔更新的方式。且更新间隔越小, 越能适用 LEO 卫星网络的高动态变化, 提供更加准确、有效的路由转发路径。

(1) 链路时延代价

由于 LEO 卫星网络中存在频繁的拓扑变化以及流量负载的不间断动态变化, 因此, 需要构建合理的星间链路时延代价, 作为路由计算代价度量。其中, 传播时延仅反映的是网络拓扑的物理连接变化, 而输出队列排队时延仅反映的是卫星网络流量变化的情况。因此, 本文选择星间链路 ISL 的传播时延与输出队列排队时延, 一同作为链路时延代价的组成因子。这样的设计保证了链路时延代价既能反映卫星网络拓扑物理连接变化, 亦能反映网络流量负载变化。

假设每颗卫星以 Δt 的时间间隔进行路由表更新。那么, 在时刻 t 进行路由更新时, 卫星节点 i 到卫星节点 j 之间的 $ISL_{i \rightarrow j}$ 的链路时延代价 $TD_{i,j}(t)$ 可以被定义为:

$$TD_{i,j}(t) = PD_{i,j}(t) + QD_{i,j}(t) \quad (3-3)$$

其中, $PD_{i,j}(t)$ 为传播时延, 具体定义如公式(3-4)所示。 $QD_{i,j}(t)$ 为输出队列排队时延, 具体定义如公式(3-5)所示。

$$PD_{i,j}(t) = \begin{cases} \frac{Dist_{i,j}}{C}, & \exists ISL_{i \rightarrow j} \\ \infty, & otherwise \end{cases} \quad (3-4)$$

其中, $Dist_{i,j}$ 代表的是卫星节点 i 到卫星节点 j 之间的物理距离。可以根据星历表的运行参数提前计算, 并将其存储在卫星上。 C 代表的是光速, 为无线或激光信号速率。若卫星节点对 i, j 之间不符合可见性的前提, 例如发生节点故障时, 则会无法建立 ISL。那么, 就将二者之间的传播时延设置为 ∞ 。

$$QD_{i,j}(t) = \frac{1}{\Delta t} \int_t^{t+\Delta t} q(y) \frac{P_{avg}}{BW} d_y \quad (3-5)$$

由于瞬时输出队列排队时延，不能较好地反映流量负载的变化。因此，通过计算在时刻 t 进行路由更新时，更新间隔 Δt 内的平均期望输出队列排队时延 $QD_{i,j}(t)$ ，来更好地反映流量负载的变化。其中， P_{avg} 为队列中数据包的平均长度， BW 代表的是 ISL 的带宽， $q(y)$ 表示在时刻 y 时，队列中的数据包数量。

(2) 链路可用带宽

星间链路可用带宽，即链路剩余带宽，为凹性度量参数。而且链路剩余带宽越大，其服务性能越好，越不易发生链路堵塞、丢包等情况。因此，在路由算法设计时，需要将链路可用带宽考虑进去。那么，星间链路可用带宽被定义为：

$$Band_{i,j}(t) = \{B_{base}(ISL_{i \rightarrow j}) - B_{used}(ISL_{i \rightarrow j})\} \quad (3-6)$$

其中， $Band_{i,j}(t)$ 为路由更新时刻 t 时，卫星节点 i 与卫星节点 j 之间的链路可用带宽。 $B_{base}(ISL_{i \rightarrow j})$ 为链路总带宽， $B_{used}(ISL_{i \rightarrow j})$ 为链路已用带宽。

(3) 链路代价修正因子

全球大多数热点是分布在赤道和 $50^\circ N$ 之间范围内^[33]的。因此，通常覆盖 $0^\circ N \sim 50^\circ N$ 区域的卫星会变得较为拥挤、繁忙。但是，其他区域卫星却未得到充分利用。由于人口分布、经济与技术发展等因素，覆盖南半球上空的卫星要比覆盖北半球上空的卫星流量负载轻得多。根据图 3-2 全球热点区域分布图显示，将南半球地区视为非热点区域。而将北半球的北美、欧洲、中东和东亚地区视为热点区域。北半球的其他地区，则被划分为非热点区域。

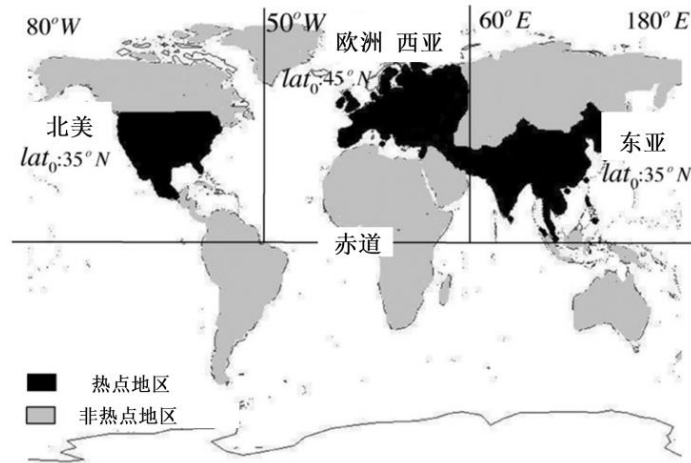


图 3-2 全球热点区域分布图

针对地面用户分布不均匀，导致全球流量分布不均衡问题。本文考虑将卫星的地理位置因素，纳入到链路代价计算中去。因此，引入了链路代价修正因子 LCF 。

那么，路由更新时刻 t 时的链路代价修正因子 $LCF_{i,j}(t)$ ，如公式(3-7)所示。以此来增强穿过热点地区的链路代价与穿过非热点地区的链路代价之间的差异性，实现将热点区域流量主动引导至非热点区域传输分散。

$$LCF_{i,j}(t) = \begin{cases} 1 & \text{if } (i = s) \\ e^{\frac{lat_i(t)}{90}} & \text{if } (0 < lat_i(t) < 50) \cap (i \neq s) \\ e^{-\frac{|lat_i(t)|}{90}} & \text{otherwise} \end{cases} \quad (3-7)$$

其中， $lat_i(t)$ 代表的是路由更新时刻 t 时，LEO 卫星 i 的纬度。 s 代表的是当 LEO 卫星 i 为源卫星节点时。

(4) 链路状态信息报告

每颗卫星在周期性间隔更新路由表项时，首先都需要获取全网链路状态数据库（Global Link State Base, GLSB）。为了方便 GLSB 的更新建立，还需将卫星链路状态报告以及轨道面的链路状态报告进行定义说明。由于构建 GLSB 过程中所涉及的星间链路相关参数，都是在路由更新时刻 t 时的。因此，为了方便后文表述，将 $TD_{i,j}(t)$, $Band_{i,j}(t)$, $LCF_{i,j}(t)$ 分别简写为 $TD_{i,j}$, $Band_{i,j}$, $LCF_{i,j}$ 。

① 卫星链路状态报告（Satellite Link State Advertisement, S_LSA）

定义卫星 i 所持有的星间链路状态信息集合为链路状态报告 $S_LSA(i)$ ，如公式(3-8)所示。

$$S_LSA(i) = \left\{ \left\langle S(m_x, n_x), TD_{i,x}, Band_{i,x}, LCF_{i,x} \right\rangle \mid \exists ISL_{i \rightarrow x} \right\} \quad (3-8)$$

其中， $S(m_x, n_x)$ 为卫星 i 的邻居卫星 x 的当前逻辑地址。

② 轨道面链路状态报告（Plane Link State Advertisement, P_LSA）

定义轨道面 m 上所有卫星的链路状态报告集合为 $P_LSA(m)$ ，如公式(3-9)所示。

$$P_LSA(m) = \{ S_LSA(x) \mid x \text{ is satellite plane } m \} \quad (3-9)$$

3.3 算法设计

本节主要对 RLQ 路由算法的具体实现展开介绍，其中包括：设计路由算法的基本思想、全网链路状态数据库的更新建立、可靠性优化路由模型的建立以及路由模型的有效求解方案。

3.3.1 基本思想

本文中，RLQ 路由算法的设计主要考虑以下两点因素：

(1) QoS 一般是对卫星网络中数据传输效果的描绘，并且是数据传递过程中不可或缺的量化指标。为了提高用户数据包在路由传输过程中的可靠性，本文设计选择综合服务性能较佳的路由转发路径来完成数据的传输，因为服务质量高的路径上其发生拥塞、丢包的概率也是较小的，能给用户带来更佳的服务体验。选择约束的 QoS 参数越多，其路径服务质量越能得到更有效、可靠的保障。但是，相应求解难度也会随之增大。因此，本文仅考虑将实际路由设计问题中最重要也是最常用的度量参数链路时延、带宽纳入进来，来完成严格多约束条件的建立，保证 RLQ 算法搜寻综合服务性能较佳的路径。

(2) 由于地面用户的不均匀分布，导致北半球上空卫星的流量负载压力要远大于南半球上空卫星。热点区域上空的卫星因流量过于集中、星上负载过大，致使星上发生拥堵，服务质量会急剧下降，大大降低了路由转发的可靠性。因此，本文将卫星地理位置因素考虑进来，提出了链路代价修正因子 LCF_{ij} 。但是，仅有修正因子是不够的，然后将修正因子与链路时延代价相融合，得到一种能够主动引导流量均衡分布的链路均衡修正代价 $Cost_{ij}$ ，如下文公式(3-10)所示。以此来减小热点区域上空卫星的压力和发生拥塞的可能性，保障卫星路由转发数据包时的 QoS，也有效提高了非热点区域上空卫星的使用率。

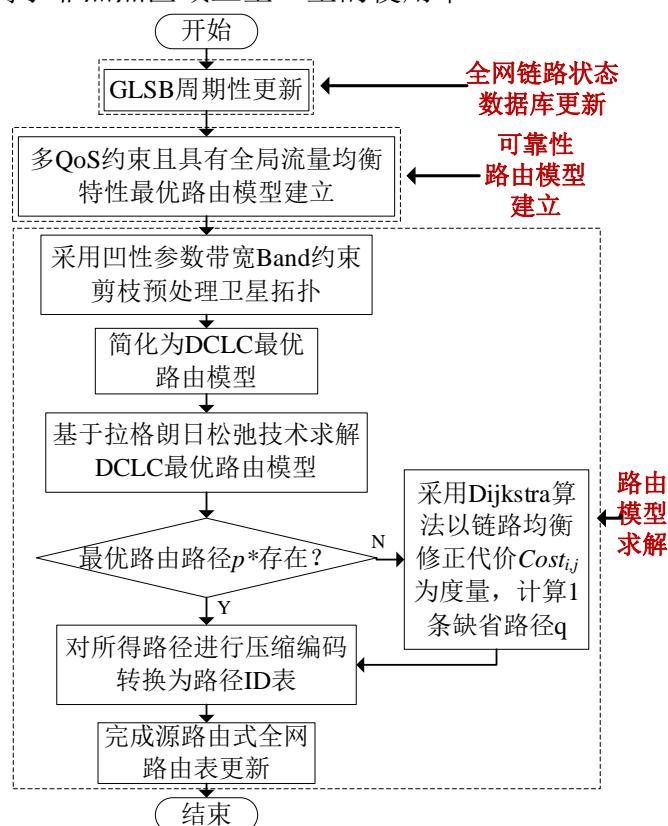


图 3-3 RLQ 算法整体运行流程

RLQ 可靠性路由算法的详细运转机制，如上图 3-3 所示。具体实现步骤为：

(1) 由于本文路由表采取的是周期性间隔更新的方式。因此，在路由表项更新时，首先需要更新每颗卫星本地所存储维护的 GLSB。

(2) 在 GLSB 基础上构建多 QoS 约束且具有流量均衡特性的最优路由模型。

(3) 为简化路由模型的求解。采用凹性参数带宽 Band 约束，对卫星网络拓扑进行剪枝预处理。将多 QoS 约束最优路由模型简化为仅有时延条件约束的最小路径代价 (Delay Constrained Least Cost, DCLC) 问题，简化后续路由模型求解。

(4) 通过基于拉格朗日松弛技术，便可求得 DCLC 最优路由模型的最优路由转发路径 p^* 。若不存在，则采用 Dijkstra 最短路径算法，以链路均衡修正代价 $Cost_{ij}$ 为度量，计算一条缺省路径 q 。

(5) 由于 RLQ 路由算法采用源路由策略。为降低路由表的存储与控制开销，因此，将计算所得的最优路径 p^* 或缺省路径 q 进行压缩编码，转换为路径 ID 表 (即路由表)，用以指导数据包的实际路由转发。

(6) 每颗卫星通过反复执行步骤 (4) - (5)，计算自己到卫星网络中其他所有卫星节点的可行路径，进而完成自身全网路由表的周期性间隔更新。

3.3.2 全网链路状态数据库更新

在更新基于 QoS 保障的全局最优路由表项时。首先，都需要 LEO 卫星网络中的每颗卫星更新本地维护的全网链路状态数据库 GLSB。在本文中采用了基于改进的轨道发言人机制，来完成对全网卫星链路状态信息的收集与分发。

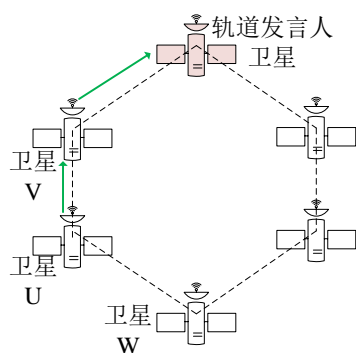


图 3-4 轨道面链路状态信息收集

首先，对于每个轨道面的链路状态信息集合 P_LSA 构建而言，是通过每个轨道面上的轨道发言人卫星完成的。每次路由更新开始时，轨道发言人卫星会收集其所处的本轨道平面内，所有其他普通卫星的链路状态报告 S_LSA ，并与自身 S_LSA 汇总后，从而形成本轨道面上全部卫星链路状态信息集合 P_LSA 。同时，每颗普通卫星会以一定频率发送自身 S_LSA 给轨道发言人卫星。

以上图 3-4 为例,解释轨道发言人卫星如何收集本轨道面内其他普通卫星链路状态信息,并生成 P_LSA 。图中卫星 U 在计算好自身链路状态信息 $S_LSA(U)$ 后,可将 $S_LSA(U)$ 发送至其相邻卫星 V 或 W 。具体发送至卫星 V 还是卫星 W ,则由卫星 V 与卫星 W 相距该轨道面内轨道发言人卫星的距离长短所决定。由卫星 V 与卫星 W 各自的地址编号,可易知哪颗距离轨道发言人卫星更近。在上图中,卫星 V 距离轨道发言人最近。那么,卫星 U 则将 $S_LSA(U)$ 发送至卫星 V 。卫星 V 在收到 $S_LSA(U)$ 后,首先会检查自己是否曾经收到过 $S_LSA(U)$ 。若收到过,则将该 $S_LSA(U)$ 丢弃。如果卫星 V 并未收到过 $S_LSA(U)$,且自身的 $S_LSA(V)$ 也尚未发送,则将自己的 $S_LSA(V)$ 连同接收到的卫星 U 的 $S_LSA(U)$ 一起发送至下一颗相邻卫星。否则,只将卫星 U 的 $S_LSA(U)$ 发送至下一颗相邻卫星。通过此种方式,在经历有限时间后,轨道发言人卫星将完整地获得本轨道面内所有其他普通卫星的 S_LSA 。同时,结合自身的 S_LSA ,形成本轨道面链路状态信息集合 P_LSA 。

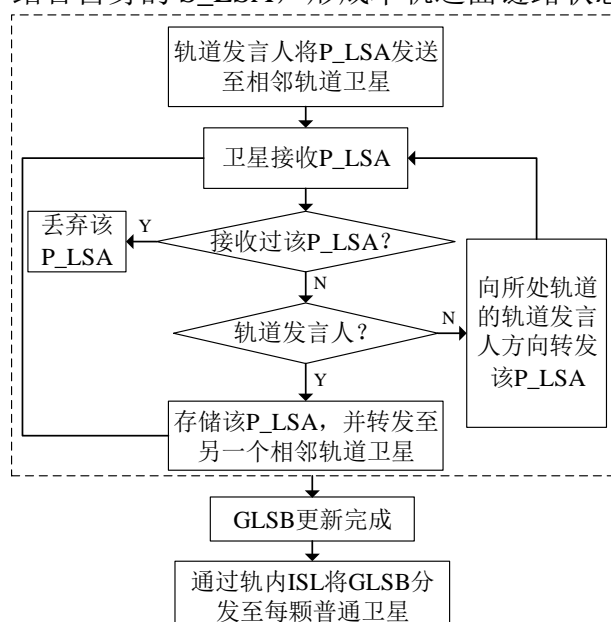


图 3-5 GLSB 更新构建

然后,对于每颗普通卫星的 GLSB 更新,也是通过轨道发言人卫星来实现的。图 3-5 详细描述了该过程。通常来说,每个轨道面上链路状态信息 P_LSA 的生成是同步进行的。当每个轨道发言人卫星完成对应轨道面的 P_LSA 生成后,轨道发言人卫星会将生成的本轨道面 P_LSA 发向相邻轨道卫星。同时,接收来自其他轨道的 P_LSA ,经过汇总之后,完成全网链路状态数据库 GLSB 的构建。每颗轨道发言人卫星在完成 GLSB 构建后,都会通过轨内 ISL 将 GLSB 分发传送至该轨道面上的每颗普通卫星。这样,LEO 卫星网络中的每颗卫星都能以较小代价开销,实现 GLSB 的周期性更新,从而为后续具体路由表项的更新计算做好准备。

最后，对于轨道发言人的实际选取，需要考虑以下两点因素：

(1) 如图 3-2 所示，全球热点区域的分布是不均匀的。覆盖南半球上空卫星的流量负载压力，要远比覆盖北半球上空的卫星轻得多。因此，应尽量使得全网链路状态数据库 GLSB 的更新，不影响热点区域上空卫星的服务质量。

(2) 考虑到在 Iridium 星座中。卫星处于极地区域时，会断开异轨间 ISL。而靠近赤道附近的卫星，其异轨间 ISL 的距离也是较长的。

因此，本文决定将轨道发言人卫星限定在由北往南飞行，且处在南半球的卫星。但是，鉴于在 Iridium 星座中，处在极地区域的卫星，会断开异轨间 ISL。若选择南半球高纬度卫星充当轨道发言人^[34]的话，虽通信时延短，但会出现因进入极地区域，轨间 ISL 断开，频繁转交轨道发言人职责的情况。故本文改进了轨道发言人的转交机制。在需进行职责转交时，将轨道发言人职责重新赋予给由北往南飞行，且处于南半球最低纬度卫星。同时，卫星是在既定轨道上作周期规律性往复运动。因此，卫星可精确得知其他卫星位置，完成轨道发言人职责转交任务。

3.3.3 可靠性路由模型建立

前文已将 RLQ 路由算法设计过程中用到的相关参数进行了定义说明。并通过在每个轨道面上设置轨道发言人卫星的方式，以较低的代价开销实现对全网链路状态信息的收集与分发，从而为网络中的每颗 LEO 卫星提供能够反映网络实时动态变化的全网链路状态数据库 GLSB。接下来，每颗 LEO 卫星就可在周期性更新的 GLSB 基础上，完成对可靠性路由模型的建模与求解。具体建模过程如下所示：

首先，为实现全球流量均衡分布，主动引导热点区域流量向非热点区域转移，降低卫星拥塞发生概率。本文将链路代价修正因子 $LCF_{i,j}$ 与链路时延代价 $TD_{i,j}$ 相融合，构造得到链路均衡修正代价 $Cost_{i,j}$ ，如公式(3-10)所示。

$$Cost_{i,j} = LCF_{i,j} \times TD_{i,j} \quad (3-10)$$

然后，为实现搜寻到的路由转发路径具有较高的服务质量。本文选择了时延与带宽两个 QoS 参数，来对路径进行严格的多 QoS 约束条件限制，保障 LEO 卫星网络提供给地面用户可靠、有效的通信基础服务。并根据公式(3-10)所设计的链路均衡修正代价 $Cost_{i,j}$ 生成最优目标函数 $\min Cost(p)$ 。

最终，得到如公式(3-11)所示的多 QoS 约束条件下，且具有流量均衡特性的最优路由模型。此路由模型搜寻到的路径 p 可实现在保证服务质量的前提下，尽量引导全球数据流量均衡分布，降低热点区域上空卫星发生拥塞的概率，减小数据传输的丢包率，提高数据传输的可靠性。

$$\begin{aligned}
 \min \text{Cost}(p) &= \sum_{(i,j) \in p(s,d)} \text{Cost}_{i,j} = \sum_{(i,j) \in p(s,d)} LCF_{i,j} \times TD_{i,j} \\
 s.t: TD(p) &= \sum_{(i,j) \in p(s,d)} TD_{i,j} \leq TD_{\max} \\
 Band(p) &= \min_{(i,j) \in p(s,d)} Band_{i,j} \geq Band_{\min}
 \end{aligned} \tag{3-11}$$

其中, s 代表源卫星节点, d 代表目的卫星节点。 $p(s, d)$ 为源-目卫星节点对之间的 1 条可行解路径, 而 $\text{Cost}(p)$ 则是所搜寻到的可行解路径 p 的链路均衡修正代价之和。 $TD(p)$ 为可行解路径 p 的累计链路时延代价之和, $Band(p)$ 为可行解路径 p 实际可用带宽值。 TD_{\max} 为用户通信业务要求的最大容忍时延, $Band_{\min}$ 为用户通信业务最小要求可用带宽。

3.3.4 路由模型求解

本节主要分为三部分进行介绍: 存在最优解时路径计算方案、不存在最优解时缺省路径计算方案, 以及对求得路径进行压缩编码得到路径 ID 表 (路由表)。

3.3.4.1 存在最优解

由于在公式(3-11)所建立的多 QoS 约束最优路由模型中, 存在着链路可用带宽 $Band_{i,j}$ 这个参数, 是一个凹性度量参数。为了降低路由模型的求解难度与复杂度, 在执行最优路由计算之前, 首先利用系统预设的最小带宽 $Band_{\min}$ 这个参数来对卫星当前所持有的 GLSB, 即全局网络状态拓扑图 $G(V, E)$ (加权有向图) 中不满足链路最小带宽 $Band_{\min}$ 约束的星间链路, 直接进行剪枝预处理操作, 进而得到剪枝预处理后新的全局网络拓扑图 $G^*(V^*, E^*)$ 。其中, V 与 V^* 代表 LEO 卫星网络中卫星节点集合, E 与 E^* 代表卫星网络中链路集合。

那么, 在新的全局卫星网络拓扑图 $G^*(V^*, E^*)$ 上搜索所需路由路径时, 将无需再考虑带宽这一约束条件。经过剪枝预处理后, 带宽 $Band_{\min}$ 这一约束条件肯定是满足的。那么, 原来公式(3-11)所设计的多 QoS 约束最优路由模型, 则变成了仅有一个时延条件约束的最小路径代价 DCLC 路由模型, 如公式(3-12)所示。 p^* 为所求最优路由转发路径, $P(s, d)$ 为源-目卫星节点对之间所有可行解路径集合。

$$p^* = \min \{ \text{Cost}(p) : p \in P(s, d) \& TD(p) \leq TD_{\max} \} \tag{3-12}$$

虽然已经删除了带宽这一约束条件, 在一定程度上降低了最优路由模型求解的难度。但是 DCLC 模型, 仍然无法在多项式时间内求出精确解, 而且其已经被证明为是一个 NP-hard 问题^[35]。因此, 本文提出采用启发式的算法来完成公式(3-12)中所示问题模型的求解, 得到问题近似解。在实际求解过程中, 本文最终选择了

采用基于拉格朗日松弛的启发式算法，来完成对最优路由路径的计算。

拉格朗日松弛算法是一种求解问题下界的方法，具有较低时间复杂度与较优计算性能。其主要思想是把约束条件吸收到目标函数中，通过减少约束条件的方式，降低原始问题计算复杂度，最终使减少约束条件后的问题能够在多项式时间内求得问题最优解。

因为拉格朗日松弛算法是一种计算目标函数下界的方法。那么，设定 $L(\theta)$ 为把时延约束条件吸收到目标函数后形成的一个新线性函数。则求解公式(3-12)所示的最优路由模型问题，被转换为下面的表达式(3-13)。其中， θ 为拉格朗日乘子。

$$L^* = \max L(\theta), \text{ 且 } \theta \geq 0 \quad (3-13)$$

$L(\theta)$ 的表达式被定义为，如公式(3-14)所示：

$$\begin{aligned} L(\theta) &= \min \{ Poly_{\theta}(p) - \theta TD_{\max} : p \in P(s, d) \} \\ &= \min \{ Poly_{\theta}(p) : p \in P(s, d) \} - \theta TD_{\max} \end{aligned} \quad (3-14)$$

$$Poly_{\theta}(p) = Cost(p) + \theta TD(p) = \sum_{(i,j) \in p(s,d)} (Cost_{i,j} + \theta TD_{i,j}) \quad (3-15)$$

其中， $Poly_{\theta}$ 为链路聚合代价 $Cost_{i,j} + \theta TD_{i,j}$ 。 $Poly_{\theta}(p)$ 为路径 p 的所包含的链路聚合代价之和，如公式(3-15)所示。同时，由拉格朗日松弛算法的相关定理^[36]证明可知， $\forall \theta \geq 0 \rightarrow Cost(p^*) + \theta TD(p^*) - \theta TD_{\max} \leq Cost(p^*)$ 。求出 θ 的值，使函数 $L(\theta)$ 取得最大值并且作为 $Cost(p)$ 的下界，那么此时所求得的路径 p ，就是满足时延 TD_{\max} 约束条件下的具有最小链路均衡修正代价之和的最优路径 p^* 。在以上公式中，当给定了 θ 的值后，就可以采用 Dijkstra 算法，完成相对应可行路径的求解。因此，为求得优化问题的下界，就需要求解得到公式(3-13)所示函数 $L(\theta)$ 的最大值。

所以，接下来通过迭代计算的方式，得到满足条件的 θ 。下面将详细介绍基于拉格朗日松弛算法的求解计算过程，具体伪代码如表 3-1 所示。

表 3-1 基于拉格朗日松弛算法的求解伪代码

算法 3-1: 拉格朗日松弛算法:

输入: $G^*, s, d, Cost_{i,j}, TD_{i,j}, TD_{\max}$

输出: 最优可行解路径 p^*

1: **Function** LARAC($G^*, s, d, Cost_{i,j}, TD_{i,j}, TD_{\max}$)

2: $p_{Cost} \leftarrow \text{Dijkstra}(G^*, s, d, Cost_{i,j})$

3: **if** $TD(p_{Cost}) \leq TD_{\max}$ **then return** p_{Cost}

4: **else** $p_{TD} \leftarrow \text{Dijkstra}(G^*, s, d, TD_{i,j})$

```

5:   if  $TD(p_{TD}) > TD_{max}$  then return “无解”
6:   else
7:     while true do
8:        $\theta \leftarrow \frac{Cost(p_{Cost}) - Cost(p_{TD})}{TD(p_{TD}) - TD(p_{Cost})}$ 
9:        $r \leftarrow \text{Dijkstra}(G^*, s, d, Poly_\theta)$ 
10:      if  $Poly_\theta(r) = Poly_\theta(p_{Cost})$  then return  $p_{TD}$ 
11:      else if  $TD(r) \leq TD_{max}$  then  $p_{TD} \leftarrow r$ 
12:      else  $p_{Cost} \leftarrow r$ 
13:    end if
14:  end while
15: end if
16: end if
17: end Function

```

在表 3-1 所示的伪代码中， G^* 为剪枝预处理后的全局网络状态拓扑图（加权有向图）。 s 表示源卫星节点， d 表示目的卫星节点。 $Cost_{i,j}$ 为链路均衡修正代价， $TD_{i,j}$ 为链路时延代价， $Poly_\theta$ 为链路聚合代价 $Cost_{i,j} + \theta TD_{i,j}$ 。 TD_{max} 为用户通信最大容忍时延。而 $\text{Dijkstra}(G^*, s, d, Cost_{i,j})$, $\text{Dijkstra}(G^*, s, d, TD_{i,j})$, $\text{Dijkstra}(G^*, s, d, Poly_\theta)$ 则分别表示使用链路均衡修正代价 $Cost_{i,j}$ 、链路时延代价 $TD_{i,j}$ 、链路聚合代价 $Poly_\theta$ 作为权重，而分别得到的源-目卫星节点对之间最短可行路径 p_{Cost} , p_{TD} , r 。

根据表 3-1，下面解释基于拉格朗日松弛的启发式算法具体计算过程：

（1）首先，令 $\theta=0$ 。此算法利用 Dijkstra 算法将链路聚合代价 $Poly_\theta$ 作为输入参数来计算最短路径。因为，当 $\theta=0$ 时，则此时计算的路径实际上是以 $Cost_{i,j}$ 为代价，计算所得的最短路径。若此时计算出的路径 p_{Cost} ，同时满足时延约束条件 TD_{max} ，则该路径 p_{Cost} 即为问题最优解 p^* ，算法终止。

（2）若步骤（1）所得路径不满足时延约束条件，算法保存第一步求解的路径 p_{Cost} 供接下来使用。然后以时延 $TD_{i,j}$ 作为 Dijkstra 的输入参数计算最短路径，若此时计算出的路径 p_{TD} 小于用户通信最大容忍时延约束 TD_{max} ，则保存该路径。否则，在当前卫星网络中，不存在满足 TD_{max} 条件约束的可行路径，算法终止。

（3）此步主要依据前两步计算所得的路径 p_{Cost} 和路径 p_{TD} ，来计算优化的 θ 值。具体实施方法则是在算法中不断迭代替换 p_{Cost} 和 p_{TD} ，直到找到满足条件的路径为止。根据拉格朗日松弛算法的性质^[36]，若存在这样的 θ 值使得 $L(\theta)$ 取得最大值，且满足 $Poly_\theta(p_{Cost}) = Poly_\theta(p_{TD})$ ，可以推导出下式：

$$\theta = \frac{Cost(p_{Cost}) - Cost(p_{TD})}{TD(p_{TD}) - TD(p_{Cost})} \quad (3-16)$$

通过将计算得出的 θ 值，带入到聚合代价函数 $Poly_{\theta}$ 中去，然后将所得的 $Poly_{\theta}$ 作为 Dijkstra 输入参数计算得出最短路径 r 。若该路径 r 满足 $Poly_{\theta}(r) = Poly_{\theta}(p_{Cost})$ ，即可求得最优路由路径 p^* 为 p_{TD} 。否则，如果 $TD(r) \leq TD_{max}$ ，则令 $p_{TD} = r$ ；如果 $TD(r) > TD_{max}$ ，则令 $p_{Cost} = r$ 。反复迭代上述计算过程，直到计算出满足条件的最优路由路径 p^* 。

本文采用拉格朗日松弛算法，对多 QoS 约束最优路由模型降维得到的 DCLC 最优路由模型进行计算。其在迭代 $O(|V|/\log|V|)$ 次后终止，而 Dijkstra 最短路径算法的时间复杂度为 $O(|V|^2)$ 。因此，基于拉格朗日松弛技术的求解算法的总时间复杂度为 $O(|V|^3 \log|V|)$ 。通过对拉格朗日乘子 θ 进行松弛，求得目标解的方式，是可以灵活控制优化目标和算法运行时间的。此算法理论上为原问题的目标函数提供了下界值，是一种求解 LEO 卫星网络下 QoS 路由的有效算法。

3.3.4.2 不存在最优解

对于 DCLC 最优路由模型的求解，如果在经过拉格朗日松弛算法计算后，没有求得最优解 p^* 。那么，就需要通过 Dijkstra 最短路径算法。在全局网络状态拓扑图 $G(V, E)$ 上，以链路均衡修正代价 $Cost_{i,j}$ 为度量代价，计算 1 条缺省路径。防止数据包路由转发进行查表时，无路由表可查询情况的发生。

3.3.4.3 路径信息压缩编码

RLQ 路由算法采用了源路由机制。同时，由于本文重点研究的是星间路由算法，着重于实现数据包从源端接入卫星到目的端接入卫星之间的逐跳传输。但是，为了更好解释两地面用户间，如何通过卫星网络进行数据的远程传递。因此，需要作如下解释说明：

当某一 LEO 卫星作为源端接入卫星，接收到源端地面用户发来的数据包时。首先，会根据数据包的目的端地面用户地址，计算出相对应的目的端接入卫星地址。然后，源端接入卫星会根据计算出的数据包目的端接入卫星地址，在每个数据包头部中，添加上完整的从源端接入卫星-目的端接入卫星节点对之间的全路径信息。中间转发卫星节点不负责路由计算，只需要依据数据包头部的路径信息进行指导，将数据包转发至下一跳卫星节点。以此类推，逐跳转发，直至将数据包转发至目的端接入卫星。最后，目的端接入卫星将数据包发送至对应的目的端地面用户即可。

同时，为了方便后文叙述。因此，决定将源端接入卫星与目的端接入卫星，分别简述为源卫星节点和目的卫星节点。

在地面传统 IP 网络中，全路径信息是由 IP 地址组成的地址序列，而 1 个 IP 地址就占用 4 个字节；在卫星网络中全路径信息可以是由卫星逻辑地址组成的地址序列。由于转发数据时需在每个数据包头部中添加全路径信息，因此给系统运行带来了较高的传输控制与存储开销。因此，为尽可能降低开销，本文引入了路径信息压缩编码机制^[32]，将计算所得的最优路径 p^* 与或缺省路径 q 转换为路径 ID 表（即路由表）。当源卫星节点有发送数据至目的卫星节点的需求时，则将自身更新维护的路径 ID 表中相对应的路径 ID 信息，添加至每个数据包的头部，指导数据包实现路由转发。中间转发卫星节点只需查询每个数据包头部的路径 ID 信息，即可将数据包按序转发至下一跳卫星节点，直至抵达目的卫星节点。路径信息压缩编码机制的设计主要分为两部分：链路 ISL 索引编码与路径 ID 表。

（1）链路 ISL 索引编码

链路 ISL 索引编码会将 1 颗卫星所维持的全部 ISL，以顺时针方向进行编码。在 Iridium 星座网络中，每颗 LEO 卫星最多维持 4 条 ISL。因此，采用 3 位二进制数字就可对其 ISL 进行编码，编码表示为 001_2 、 010_2 、 011_2 、 100_2 。且每颗 LEO 卫星都须在星上维护 1 个链路 ISL 索引编码表，如图 3-6 所示。

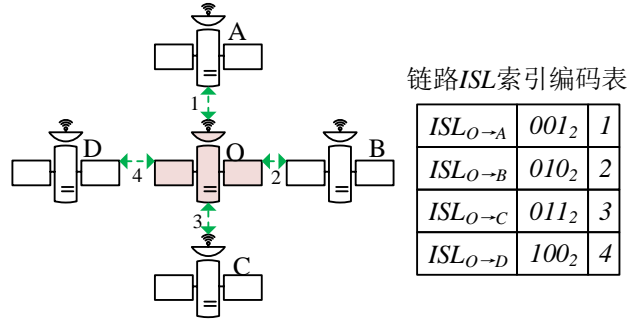


图 3-6 Iridium 星座链路 ISL 索引编码

（2）路径 ID 表

源-目卫星节点对之间的 1 条可行解路径（最优路径解 p^* 或缺省路径解 q ），可被转换为由链路 ISL 索引编码值反向顺序所构成的有序二进制序列，记为 1 条可行解路径的路径 ID 信息，并被具体表示为 P_ID ，如公式(3-17)所示。

$$P_ID = [ISL_{index_xxx} + ISL_{index_xxx} \dots] \quad (3-17)$$

其中， P_ID 最左侧 ISL_{index_xxx} 代表的是，连接目的卫星节点的链路 ISL 的索引编码。

每颗卫星会周期性更新维护自己到网络中其他所有卫星节点的路径 ID 信息 P_ID 。那么，所有的 P_ID 可构成路径 ID 表（即路由表）。如表 3-2 所示。

表 3-2 路径 ID 表结构

目的卫星节点地址	路径 ID 信息
Dest_Satellite_ID ₁	P_ID ₁
Dest_Satellite_ID ₂	P_ID ₂
...	...
Dest_Satellite_ID _{num}	P_ID _{num}

当某一颗 LEO 卫星作为源卫星节点，并有数据发送任务时。那么，就根据计算出的数据包目的卫星节点地址 Dest_Satellite_ID，从本地存储周期性更新维护的路径 ID 表中，选择相对应的路径 ID 信息 P_ID，将其添加至数据包头部。用以指导数据包的实际路由转发，简化中间卫星节点的转发过程。

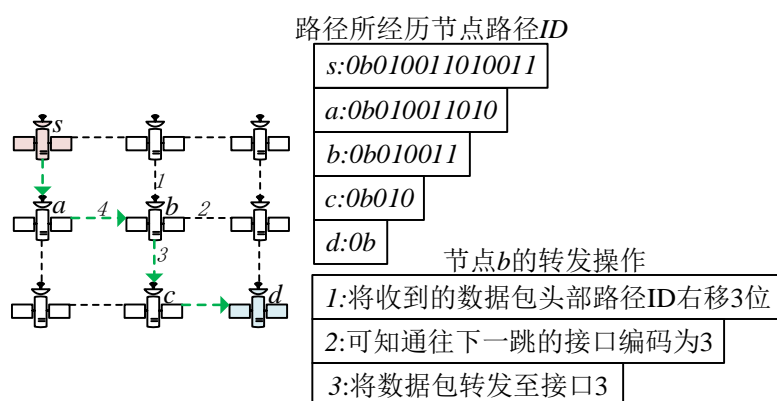


图 3-7 编码与数据包转发示意图

在 LEO 卫星网络中采用路径 ID 表指导数据包转发过程，如上图 3-7 所示。当某一中间转发卫星节点收到一个数据包时。首先，会提取出数据包头部的路径 ID 信息 P_ID。依据路径 ID 最右侧的 3 位，查找自身链路 ISL 索引编码表。然后，将数据包的路径 ID 右移 3 位后，重新添加至数据包头部。最后，将数据包转发至索引编码相对应的出口链路。

图 3-7 中绿色箭头所指示的路径为源 s -目的 d 卫星节点对之间的 1 条可行解路径。源卫星节点 s 首先会将数据包转发至下一跳卫星 a 。此时，数据包所持有的路径 ID 为 010011010₂。卫星 a 接收到此数据包后，依据路径 ID 最右侧 3 位 (010₂) 可知，应将数据包转发至卫星 a 自身索引为 2 的接口。那么，数据包接着就可以被发送至卫星节点 b 。同时，数据包的路径 ID 会被右移 3 位重置。以此类推，后续中间转发卫星节点执行同样的操作，直至将数据包转发至目的卫星节点 d 。

3.4 仿真设计及结果分析

本节将采用 NS2^[37-38]网络仿真软件,来完成对本文所提出的 RLQ 路由算法与文献[15]提出的基于虚拟拓扑最短路径思想的 DT-DVTR 路由算法、文献[18]提出的显式流量均衡 ELB 路由算法之间,在平均端到端时延、丢包率,以及网络整体吞吐量、流量均衡指数、归一化链路负载等方面的性能对比仿真。

3.4.1 仿真环境和参数设置

由于 STK^[39]卫星仿真软件不支持卫星网络路由算法的仿真。而 OPNET^[40]网络仿真软件的使用成本较高。且对其网络底层构件的修改,也较为困难。因此,本文决定使用免费开源的、面向对象基于离散事件驱动的 NS2 网络仿真软件,来完成对各 LEO 卫星网络路由算法的仿真测试。NS2 目前支持极轨道卫星星座的仿真实现,且 NS2 是采用 2 种面向对象的语言来完成开发实现:C++与 OTcl。本文是在 NS2 所提供的卫星网络仿真基础之上,修改了部分代码,来完成实现各卫星网络路由算法:RLQ 路由算法、DT-DVTR 路由算法以及 ELB 路由算法。通常 NS2 的网络仿真流程,如图 3-8 所示。

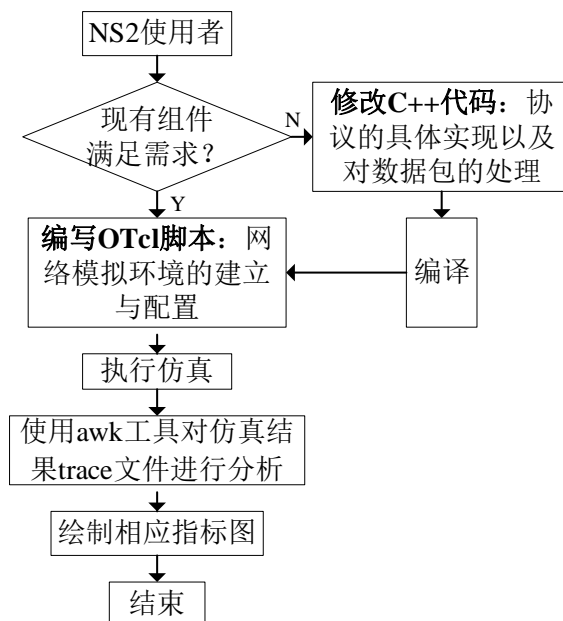


图 3-8 NS2 网络仿真流程

采用 NS2 进行网络仿真时,需要对各仿真参数进行详细设定。

首先,关于地面用户终端选择接入卫星的方式。设定地面用户终端根据最长覆盖时间的原则,来决定接入卫星。同时,设定地面用户终端每隔 10s,对其服务卫星的最小仰角进行检查。若不满足,则及时进行接入卫星的切换。

其次，对地面用户终端呼叫 QoS 性能要求进行设定。如表 3-3 所示。

表 3-3 呼叫 QoS 性能要求

参数	数值
最小可用带宽要求 $Band_{min}$ (kb/s)	200
最大容忍时延要求 TD_{max} (ms)	200

接下来，对地面用户终端的仿真参数进行设定，如表 3-4 所示。产生服从 Pareto 分布的 on/off 数据流。同时，需要对 Iridium 星座的仿真参数进行设定，如表 3-5 所示。

表 3-4 地面用户终端仿真参数

核心参数	数值
仿真时间 (s)	6060
数据包大小 (Bytes)	1000
“on” 周期 (s)	0.4
“off” 周期 (s)	0.8
“on” 周期内数据发送速率 (kb/s)	200~1200

表 3-5 Iridium 星座仿真参数

核心参数	数值
高度 (km)	780
轨道面数	6
单轨道面卫星数	11
最小仰角	8.2°
轨道倾角	86.4°
极区阈值	70°
ISL 队列类型	FIFO
ISL 队列长度 (Packets)	400
ISL 带宽 (Mb/s)	10
UDL 带宽 (Mb/s)	10

然后，为了模拟 Iridium 星座网络中真实的流量分布情况。通过基于人口密度因素，在地面设置分布 300 个通信终端。源终端和目的终端在地面的分布情况，服从^[41]表 3-6。

表 3-6 地面终端分布情况 (%)

源终端	目的终端					
	北美	南美	欧洲	非洲	亚洲	大洋洲
北美	60	10	15	2	10	3
南美	35	40	12	2	8	3
欧洲	40	5	40	2	10	3
非洲	40	2	30	20	5	3
亚洲	30	2	10	2	50	6
大洋洲	40	2	10	2	12	34

最后，在 RLQ 路由算法中，设定全网链路状态数据库 GLSB 每隔 20s 进行一次更新。因此，路由表周期性更新间隔也为 20s。通过设置不同的终端发送速率，将本文所提出的 RLQ 路由算法与 DT-DVTR 路由算法以及 ELB 路由算法。在平均端到端时延、丢包率，以及网络整体吞吐量，流量均衡指数、归一化链路负载情况等方面，进行统计对比分析。

3.4.2 仿真结果分析

(1) 平均端到端时延

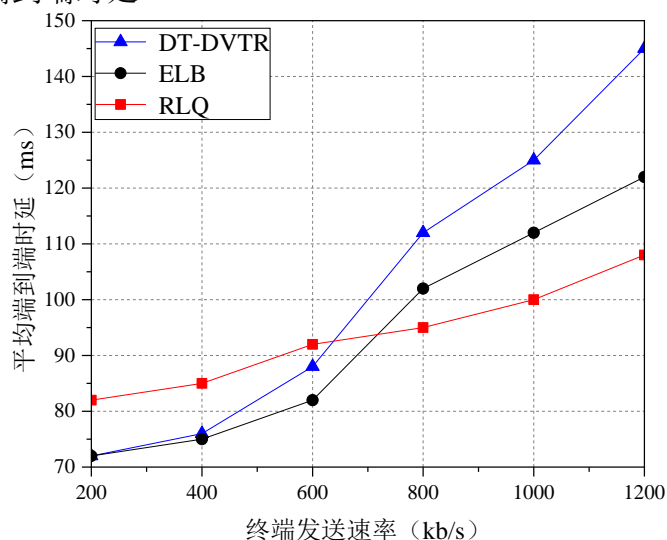


图 3-9 平均端到端时延随终端发送速率变化曲线图

平均端到端时延可由整个网络中所有端到端通信时延，求平均得到。由图 3-9 可知。随着终端发送速率的不断增大，RLQ 算法、ELB 算法以及 DT-DVTR 算法的平均端到端时延均在上升。这是由于终端发送速率的提高使得网络负载变重，输出队列排队时延上升导致的。在终端发送速率低于 600kb/s 网络负载较轻时，

DT-DVTR 算法与 ELB 算法的时延均低于 RLQ 算法, 此时是由于 RLQ 算法为实现流量从热点区域向非热点区域主动分散, 因此经历了更多的传输跳数, 导致时延较大; 在终端发送速率高于 600kb/s 网络负载较重时, DT-DVTR 算法依旧选择最短路径完成路由转发, 并没有考虑最短路径上节点和链路的资源占用情况, 导致排队时延陡增, 端到端时延性能最差。ELB 算法虽然在路径计算时没有考虑输出队列排队时延, 但是其在节点即将拥塞时, 会主动发送拥塞通知告知上游节点, 以降低对此节点的数据发送量, 并计算一条不包含该拥塞节点的新路径, 实现流量分流。因此, 端到端时延增加平缓一些。但若在一定时间内找不到分流路径, 节点便会很容易拥塞, 增大排队时延。而且 ELB 仅在局部范围实现流量均衡, 故效果欠佳。而本文所提出的 RLQ 路由算法在网络负载较重时表现出了极佳的时延性能。因为 RLQ 算法在路径选择时不仅考虑了节点队列占用情况, 即排队时延, 而且对其进行了时延、带宽等多 QoS 条件约束。并从网络全局角度出发, 实现流量的主动分散, 使得网络流量负载在全网分布较为均匀, 节点资源占用率较低, 排队时延较小。因此, 保证了路由转发时具有较佳的端到端时延性能。

(2) 丢包率

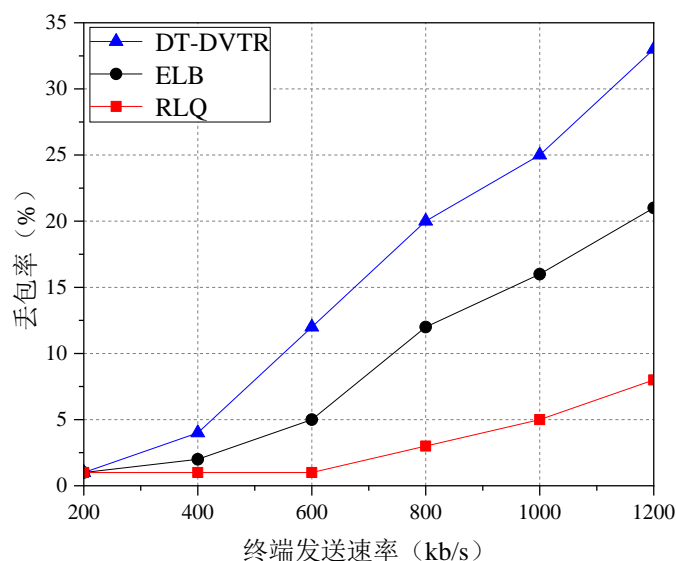


图 3-10 丢包率随终端发送速率变化曲线图

丢包率指的是未成功交付给目的终端的数据包个数与所有源终端发出的数据包总数比值。由图 3-10 可知。随着终端发送速率的不断增大, RLQ 算法、ELB 算法以及 DT-DVTR 算法的丢包率均在增加。这是由于终端发送速率的提高, 使得转发路径上的卫星发生拥塞, 队列溢出数据包导致的。其中, DT-DVTR 算法的表现最差。因为, 其在数据转发时仅选择最短路径, 并没有考虑节点资源占用情况; ELB 算法在终端发送速率超过 400kb/s 时, 丢包率性能逐渐下降, 但是优于

DT-DVTR 算法。虽然通过拥塞通知上游节点降低发送速率以及计算备份路径的方式，一定程度上实现了流量的局部均衡。但是随着终端发送速率的不断增大，ELB 算法运行时所需要的拥塞通知包也会大量产生，进一步恶化路径的拥塞程度。因此，丢包率也较为严重；而本文所提出的 RLQ 算法，是在保障路径服务质量 QoS 前提下，尽量引导流量实现全球均衡分布的，因此，路径中节点资源占用率低，节点发生拥塞的概率也低。因此，具有最小的丢包率，保证了路由转发的可靠性。

(3) 网络吞吐量

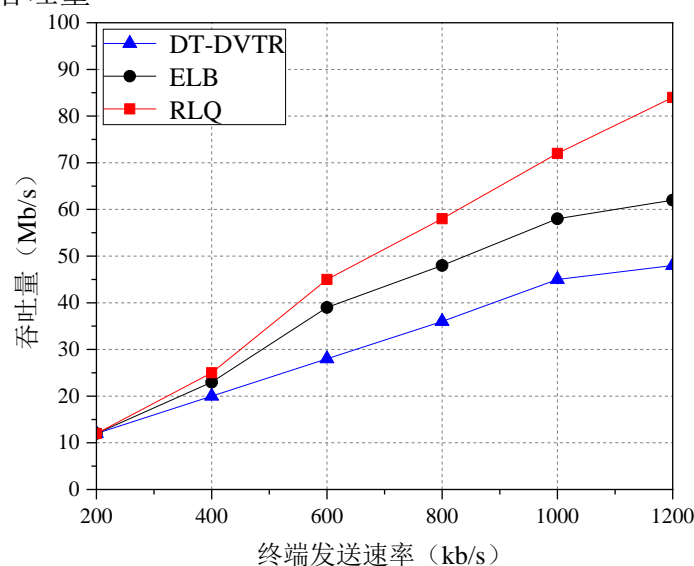


图 3-11 网络吞吐量随终端发送速率变化曲线图

网络吞吐量指的是，单位时间内网络传输的数据量大小。且卫星网络整体吞吐量越高，代表卫星网络路由的数据传输能力越强劲。图 3-11 描述的是网络吞吐量随终端发送速率变化的曲线图。在终端发送速率低于 400kb/s 时，三者吞吐性能大致相当；可是随着终端发送速率的进一步增加，RLQ 算法的吞吐性能表现最佳，因为 RLQ 算法是从网络全局角度，实现流量的均衡分布，且在路径选择时进行了多 QoS 条件约束。虽然经历了更多的传输跳数，但是使得网络整体中节点以及链路负载较低，发生拥塞的概率较小，丢包也较少。因此，吞吐性能最佳。而 ELB 算法在网络拥塞时，会发送大量拥塞通知包。因此，使得传输路径更加拥塞，造成了队列溢出数据包的丢失。DT-DVTR 算法的吞吐性能表现最差，这与它只选择最短路径进行数据传输密切相关，没有实现流量的均衡传输。

(4) 流量均衡指数

为衡量各路由算法在流量均衡方面的表现。因此，引入了流量均衡指数^[19] F_{index} 来体现星座网络中整体流量分布情况，如公式(3-18)所示。其中， F_{index} 的取值范围为[0, 1]， F_{index} 值越大，流量均衡表现越好。 n 代表的是 ISL 条数， x_k 代表的是经

过第 k 条 ISL 的数据包总数。

$$F_{index} = \frac{(\sum_{k=1}^n x_k)^2}{n \sum_{k=1}^n x_k^2} \quad (3-18)$$

图 3-12 描述的是流量均衡指数 F_{index} 随终端发送速率变化的曲线图。由图易知，本文所提出的 RLQ 算法具有最佳的流量均衡效果，因为 RLQ 算法是从网络全局角度主动引导热点流量向非热点转移，既分担了热点区域上空卫星压力，也使得非热点区域上空卫星的使用率也有所增加。因此，全网流量分布较为均匀；ELB 算法的流量均衡表现略差于 RLQ 算法，因为其仅在局部范围内实现流量均衡；而 DT-DVTR 由于仅使用最短路径进行数据传输，并没有考虑流量均衡问题。因此，流量均衡效果最差。

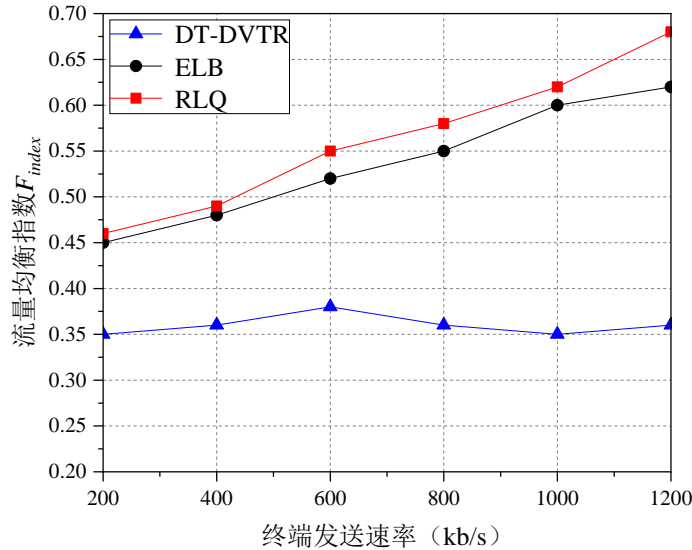


图 3-12 流量均衡指数 F_{index} 随终端发送速率变化曲线图

(5) 归一化链路负载

为观测卫星负载跟卫星所处纬度位置的关系。因此，定义了归一化链路负载指标^[42] ISL_{load} ，如公式(3-19)所示。其中， $Total_{traffic}$ 代表的是流经卫星总流量， $Total_{band}$ 代表的是 ISL 总带宽， T_{period} 代表的是一个时间段。

$$ISL_{load} = \frac{Total_{traffic}(Mb)}{T_{period}(s) \times Total_{band}(Mb/s)} \quad (3-19)$$

设定终端发送速率为 400kb/s，使得卫星网络处于轻度拥塞状态下，观测 1 颗指定卫星绕地运行一圈过程中，卫星处于不同纬度位置时 ISL_{load} 情况，如图 3-13 所示。可知本文提出的 RLQ 算法实现了流量的主动分散，在热点区域时 ISL_{load} 要

小于 DT-DVTR 算法与 ELB 算法，而在非热点区域时 RLQ 的 ISL_{load} 要大于另外两者。并且三者路由算法均在 $30^{\circ}N$ 时 ISL_{load} 达到了顶峰值，这符合全球热点区域分布规律。在热点区域时由于 ELB 算法的局部负载均衡效果。因此，其 ISL_{load} 要小于 DT-DVTR 算法，但仍不如 RLQ 算法全局流量均衡所带来的有益之处。

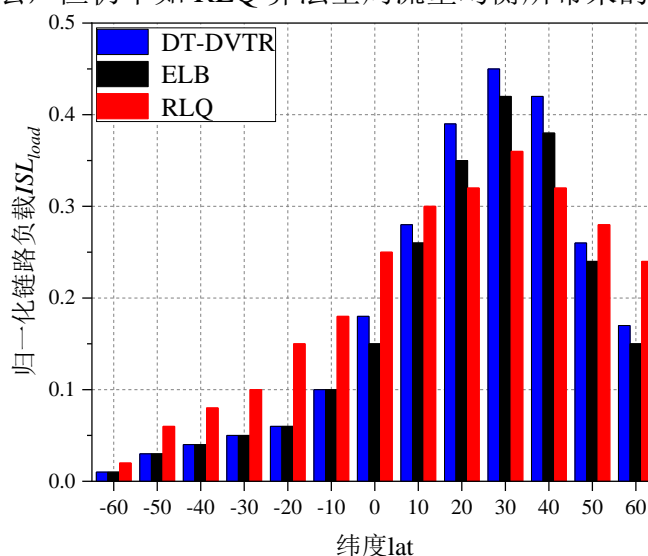


图 3-13 卫星处于不同纬度位置时 ISL_{load} 情况

3.5 本章小结

为实现空间段路由转发路径具有较优的服务质量，以及实现全球流量的主动均匀分布，本章从 QoS 保障为切入点，提出设计了一种 RLQ 可靠性路由算法。首先，采用一种改进的轨道发言人机制完成 GLSB 的更新；然后，考虑时延、带宽等约束条件以及地面用户分布不均等因素后，提出一种多 QoS 约束的且具有流量均衡特性的最优路由模型；接下来，通过剪枝预处理以及基于拉格朗日松弛技术完成对最优可行解路径的求解，并采用路径信息压缩编码机制得到用以指导实际数据包路由转发的路径 ID 表；最后，采用 NS2 网络仿真软件，来完成 RLQ 路由算法与 DT-DVTR 路由算法、ELB 路由算法之间，在平均端到端时延、丢包率、吞吐量、流量均衡指数以及归一化链路负载等方面的性能对比分析，RLQ 算法均取得了不错的性能表现。

第四章 基于节点信任度的 LEO 卫星网络安全路由算法

4.1 引言

LEO 卫星通信系统作为未来 6G 通信时代发展的重要一员,因其兼备通信时延小、覆盖范围广以及发射成本较低等优势,已经受到各国航天研发领域的重点扶持与青睐。未来太空中,将会有更多的 LEO 卫星通信系统为实现万物互联,提供实时、有效的基础网络转发服务。

但是,LEO 卫星通信系统又同时具有无线通信媒介开放、高动态拓扑变化、分布式协作以及卫星节点资源受限等特性,这就增加了对路由算法的设计难度。暴露在复杂空间环境中的 LEO 卫星的 ISL,由于受其自身稳定性差、开放性、暴露性等特点的影响。故易受到来自恶意节点的干扰与攻击。而卫星网络的路由协议则恰恰是诸多攻击行为的首选目标,使得空间中的数据传输面临极大的安全威胁与挑战。具体的攻击分类可按照恶意节点与 LEO 卫星网络的关系进行划分,分为外部攻击与内部攻击。

(1) 外部攻击指的是网络外部的恶意节点,对卫星网络内部的节点开展窃听与压制等行为的攻击。对于来自卫星网络外部的各类攻击,通过传统的基于密码学的安全技术方案就能得到有效的解决防护^[25-26]。

(2) 内部攻击指的是卫星网络中的正常节点被恶意节点劫持并篡改,从而再以合法身份重新入网,在卫星网络内部发动诸如黑洞、灰洞等方式的攻击行为^[43]。黑洞卫星节点,会完全丢弃收到的全部数据包。灰洞卫星节点,则只会丢弃收到的部分数据包。

然而,此种从网络内部发起的攻击行为,传统基于密码学的安全技术方案却无计可施,无法继续保障路由安全性。而信任管理对于解决网络内部攻击却有较为出色表现。对从网络内部发起攻击的恶意节点,进行及时有效地检测识别与隔离处置,最大程度降低恶意卫星节点对于星间数据传输的恶劣影响。因此,本文针对从卫星网络内部所发起的路由攻击行为,兼顾 LEO 卫星网络内在特点和基于信任管理的安全加固理念,提出了一种基于节点信任度的 LEO 卫星网络安全路由算法(Secure routing algorithm of LEO satellite network based on node Trust, SLT)。

本章的主要贡献如下:

(1) 基于 D-S 证据理论,设计了一套不需要任何集中式或分布式可信基础措施,通过卫星节点的分布式协作,就可实现节点信任度更新的 LEO 卫星网络动态信任评估模型。其中,包括直接信任、间接信任以及聚合信任模型的设计。

(2) 采用本章所提出的此套信任评估模型, 对一种低开销基于轨道预测的 LEO 卫星网络路由协议 (Orbit Prediction Shortest Path First Routing for Resilient LEO Satellite Networks, OPSPF^[44]) 进行安全信任加固改造, 设计出 SLT 安全路由算法, 以此来增强空间数据传输的安全性与可靠性。其中, 包括基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块的设计。

4.2 基于 D-S 证据理论的 LEO 卫星网络信任评估模型

目前, 针对 LEO 卫星网络所研究的路由算法, 大多数是以服务质量 QoS 为路由度量进行设计的, 仅少数研究在路由决策时考虑了路由转发路径的安全性。而对于从网络内部发起的攻击, 信任管理方案具有极佳的处理优势。为实现基于信任加固的 LEO 卫星网络安全路由算法, 首先需要提出一种合理、可行的信任评估模型。通过信任评估模型, 进行恶意卫星节点的实时监测与有效识别。

但是, 因为 LEO 卫星网络可看成是一种特殊的、具有规律运动特点的空间移动 ad hoc 分布式网络, 且距离地面较远。难以实现像在地面通信网络中, 通过第三方可信机构, 便可实现集中式的网络全部节点的信任值计算。因此, 需要通过节点间的相互协作认证, 来构建分布式的动态信任模型, 计算 LEO 卫星网络中各卫星节点的信任值。可是, 已有信任模型却不能直接应用于 LEO 卫星网络。由于卫星网络拓扑频繁变化和无线冲突发生, 用于评估信任的证据抽样空间可能会不完全或不可靠。幸运的是, Dempster-Shafer(D-S)证据理论^[45-46], 可处理信任评估中的随机性与主观不确定性。通过证据的不断积累, 可在无先验分布条件下, 减小假设集, 为信任的不确定性表达和处理提供可行方法。

因此, 综合以上多因素考虑。本文基于 D-S 证据理论, 提出设计了一种不需要任何集中式或分布式可信基础措施, 通过卫星节点的分布式协作, 便可实现节点信任度更新的 LEO 卫星网络信任评估模型, 如图 4-1 所示。

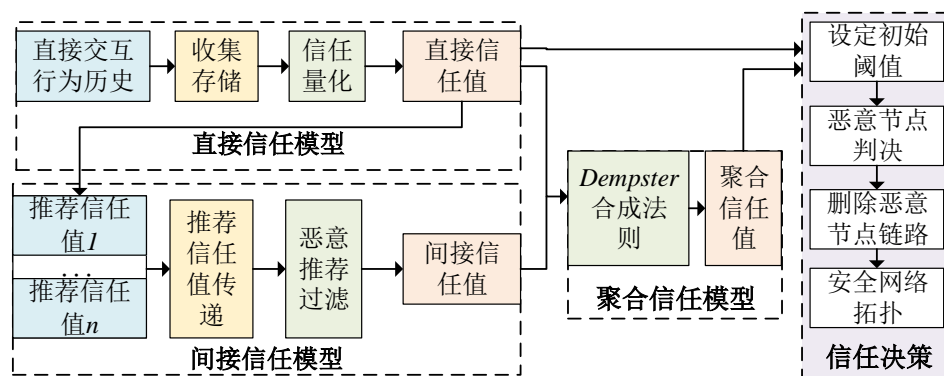


图 4-1 基于 D-S 证据理论的 LEO 卫星网络的信任评估模型

在 LEO 卫星网络的协同服务模型中, 信任的主客体都是参与星间组网通信的 LEO 卫星。信任是一颗卫星对其他卫星能否正确完成对应网络服务的主观可能性预测。该卫星所监测统计到的目标卫星行为, 与其他卫星对目标卫星的推荐信息, 则是预测的基础来源。两种信任关系可称为直接信任与间接信任, 进一步也可得到聚合信任。最终, 就可以依据相应信任评估模型, 得到一个卫星节点对其邻居转发卫星节点的信任程度。

本节主要分为四部分开展介绍: D-S 证据理论知识、直接信任模型、间接信任模型以及聚合信任模型。对于信任决策的处理部分则在 4.3.3 节中进行描述。

4.2.1 D-S 证据理论知识

由于本文采用了基于 D-S 证据理论知识, 来完成对 LEO 卫星网络动态信任评估模型的设计。因此, 需要对 D-S 证据理论的基础定义, 以及 Dempster 合成法则进行简要说明。

4.2.1.1 基础定义

假定 Ω 是由 N 个互斥且穷举的基本命题所构成的有限集合, 则将 Ω 称为辨识框架。

Ω 的幂集 $P(\Omega)$ 是由 2^N 个关于 Ω 的全部可能子集所组成的集合, 记作 $P(\Omega) = \{\emptyset, \{A_1\}, \dots, \{A_2\}, \{A_1, A_2\}, \{A_1, A_3\}, \dots, \Omega\}$, 其中, \emptyset 代表的是空集。在 $P(\Omega)$ 上设计了一个基本置信度函数 (Basic Probability Assignment, BPA) $m(A): P(\Omega) \rightarrow [0, 1]$, 代表的是对 A 的信任程度, 满足公式(4-1):

$$\begin{cases} \sum_{A \subseteq P(\Omega)} m(A) = 1 \\ m(\emptyset) = 0 \end{cases} \quad (4-1)$$

信任函数 Bel , 表示对某一集合及其全部子集总信任度。可设计成 $Bel(A): P(\Omega) \rightarrow [0, 1]$, 满足公式(4-2):

$$Bel(A) = \sum_{B \subseteq A} m(B), \forall A \subseteq P(\Omega) \quad (4-2)$$

似然函数 Pl , 表示对命题 A 不否定程度。可设计成 $Pl(A): P(\Omega) \rightarrow [0, 1]$, 并且满足公式(4-3)。并跟信任函数 Bel 之间满足: $Pl(A) = 1 - Bel(\neg A)$ 。且 $\neg A$ 为 A 的否命题。

$$Pl(A) = \sum_{A \cap B = \emptyset} m(B), \forall A \subseteq P(\Omega) \quad (4-3)$$

4.2.1.2 Dempster 合成法则

定义在同一个辨识框架 Ω 的前提下, 拥有 $n(n \geq 2)$ 个互斥且穷举证据, 设计它们基本置信度函数为 m_1, m_2, \dots, m_n 。采用 Dempster 合成法则, 可将这 n 个证据进行合成, 得到基本置信度函数为 $m(A)$, 并且需要符合以下约束:

$$\begin{cases} m(\emptyset)=0, A \subset P(\Omega) \\ m_1(A) \oplus m_2(A) = \frac{\sum_{X \cap Y=A} m_1(X)m_2(Y)}{1-K} \\ K = \sum_{X \cap Y=\emptyset} m_1(X)m_2(Y) \\ m(A) = ((m_1(A) \oplus m_2(A)) \oplus \dots) \oplus m_n(A) \end{cases} \quad (4-4)$$

其中, K 称为冲突因子, 可反映不同 BPA 两者之间的冲突剧烈程度。

满足交换性与结合性, 也是 Dempster 合成法则所具有的特点之一。例如满足 $m_1 \oplus m_2 = m_2 \oplus m_1$, 以及 $(m_1 \oplus m_2) \oplus m_3 = m_1 \oplus (m_2 \oplus m_3)$ 。

定义 m_1 与 m_2 为同一辨识框架 Ω 下的 2 个不同 BPA, 则定义 m_1 与 m_2 之间的距离 $z(m_1, m_2)^{[47]}$ 为:

$$z(m_1, m_2) = \sqrt{\frac{1}{2} (\|m_1\|^2 + \|m_2\|^2 - 2\langle m_1, m_2 \rangle)} \quad (4-5)$$

其中, $\langle m_1, m_2 \rangle$ 为 m_1 与 m_2 之间的数量积, 如公式(4-6)所示:

$$\langle m_1, m_2 \rangle = \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} m_1(A_i) m_2(A_j) \left| \frac{A_i \cap A_j}{A_i \cup A_j} \right| \quad (4-6)$$

其中, $A_i, A_j \in 2^\Omega$, $\|m\|^2$ 为 m 平方范式。那么, $\|m\|^2 = \langle m, m \rangle$ 。

4.2.2 卫星网络直接信任模型

在 LEO 卫星通信网络系统中, 若一个卫星节点与其他卫星节点正常交互次数越多, 则表明该卫星节点的可信程度越高, 其发生恶意行为的可能性越低。因此, 本文根据一个卫星节点是否能正确转发数据包, 来评价该节点的可靠性程度。卫星节点可以根据之前在本地监测、收集存储的直接交互行为历史, 来计算对其他卫星节点的直接信任。

由于在 LEO 卫星通信网络这种特殊的网络环境下, 不适宜采用集中式通过第三方可信机构, 来完成卫星节点信任值的计算。因此, 本文采用了一种通过卫星节点间分布式协作的方式, 来计算卫星节点的信任值。一个卫星节点对其邻居转发卫星节点进行信任评估时, 需要统计其数据包历史转发行为。因此, 为统计被

评估卫星节点的数据包转发行为，本文引入了一种两跳回复消息机制^[48]。若信任评估主体卫星节点，在设定等待时间内收到了两跳回复消息，则表明被评估邻居卫星节点已经成功将数据包转发。具体的数据包发送判决流程示例，如图 4-2 所示。

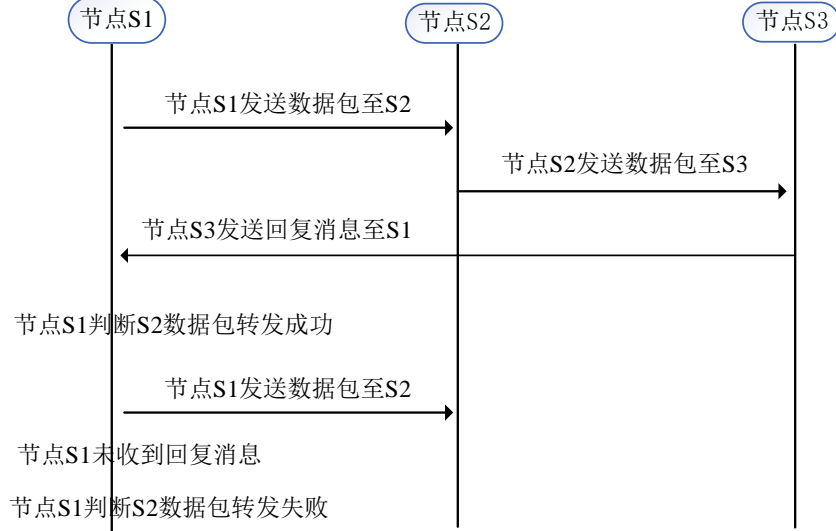


图 4-2 数据包发送判决过程

两跳回复消息的格式如图 4-3 所示。其中， $S_address$ 为消息发送卫星节点地址； $F_address$ 为数据包转发卫星节点地址； $D_address$ 为数据包目的卫星节点地址； $Signature_information$ 是对上述信息哈希值的签名验证消息。

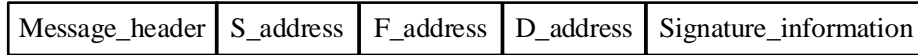


图 4-3 回复消息报文格式

通过上述方法，卫星节点可对邻居转发卫星的数据包转发行为进行统计判断，为直接信任的量化提供基础。设卫星节点成功转发数据包行为的次数为 $N_{success}$ ，卫星节点失败转发数据包行为的次数为 N_{fail} 。

$$\begin{cases} a = \frac{N_{success}}{N_{success} + N_{fail}} \\ b = \frac{N_{fail}}{N_{success} + N_{fail}} \\ \text{且 } 0 \leq a, b, c \leq 1, a + b + c = 1 \end{cases} \quad (4-7)$$

依据上述分析，接下来，本文首先根据 D-S 证据理论，设定了一个辨识框架 $\Omega = \{T, \sim T\}$ 。其中， T 表示信任， $\sim T$ 表示不信任。同时，采用一个向量 SD 对卫星节点的直接信任进行表示， $SD = (m(\{T\}), m(\{\sim T\}), m(\{T, \sim T\}))$ 。其中， $m(\{T\})$,

$m(\{\sim T\})$, $m(\{T, \sim T\})$ 各自代表的是数据包被成功转发的概率比值、数据包被明显拒绝转发概率比值, 以及对于是否成功转发数据包不确定的概率比值。其值各自采用 a, b, c 进行表示, 由公式(4-7)求得。同时, 一个卫星节点对其邻居转发卫星节点的直接信任值会被存储在本地, 以备后续安全信任决策时调用。

在 LEO 卫星通信系统中, 信任是具有动态性变化的特点。通俗来讲, 就是说信任关系是会随时间和环境而不断动态变化的, 并不是一成不变的。一个卫星节点对于其某一个邻居转发卫星过去的信任, 并不意味着现在亦或是将来还会继续信任。邻居转发卫星节点一些行为或者其他的一些相关信息, 会导致该卫星不再信任其邻居卫星节点, 所以需要设计一种动态的信任评估模型, 能够准确反映这种动态性变化, 也要具备信任会随时间和环境变化而重新计算评估的能力^[49]。

考虑到信任的动态性变化特点。因此, 本文决定在时域上开展卫星节点信任值的研究。在系统最初运行时, 卫星节点 i 与卫星节点 j 之间由于无交互历史统计。所以, 此时刻卫星节点 i 对卫星节点 j 的直接信任向量 $SD_{i,j}(t_0)=(0, 0, 1)$ 。设定卫星节点更新其直接信任向量 SD 的周期为 Δt , 所以当 $t=t_n$ 时, $SD_{i,j}(t_n)=(a_n, b_n, c_n)$, a_n, b_n, c_n 各自代表的是 t_n 时, 数据包被成功转发的概率比值、数据包被明显拒绝转发概率比值以及对于是否成功转发数据包不确定的概率比值。在经过 Δt 间隔以后, 即 $t=t_{n+1}=t_n+\Delta t$, $SD_{i,j}(t_{n+1})=(a_{n+1}, b_{n+1}, c_{n+1})$ 。为阻止恶意卫星节点快速提高自己的信任值, 卫星节点 i 按照如公式(4-8)所示的方式, 进行更新自己对节点 j 的直接信任值。

$$\begin{aligned} SD'_{i,j}(t_{n+1}) &= (1-w)SD_{i,j}(t_n) + wSD_{i,j}(t_{n+1}) = (a'_{n+1}, b'_{n+1}, c'_{n+1}) \\ &= (m_{i,j}(\{T\}), m_{i,j}(\{\sim T\}), m_{i,j}(\{T, \sim T\})) \end{aligned} \quad (4-8)$$

其中, w 代表的是 1 个权重因子 (常量)。并且在更新信任证据的过程中, 权重因子 w 的值, 将会被卫星节点 i 动态选定, 如公式(4-9)所示。

$$w = \begin{cases} w_1, & \text{if } ((a_{n+1} - a_n) \geq (b_{n+1} - b_n)) \\ w_2, & \text{if } ((a_{n+1} - a_n) < (b_{n+1} - b_n)) \end{cases} \quad (4-9)$$

其中, w_1 与 w_2 满足约束: $0 \leq w_1 \leq 0.5 \leq w_2 \leq 1$ 。通过这种对 w 值进行动态选取的方法, 来实现对不同卫星节点表现“赏罚分明”。且 $w_1 < w_2$ 说明惩罚力度强于奖励力度。通过此策略, 既做到了对优质卫星节点的奖励, 亦做到了对恶意卫星节点的严惩, 减少卫星节点的恶意行为, 也能够有效抑制恶意卫星节点迅速提高自身信任值。

通过以上操作, 卫星节点 i 便可以实现对邻居转发卫星节点 j 的准确合理直接信任度量, 即完成对直接信任值的更新, 也对 LEO 卫星网络的实时变化做出了及时有效地动态响应。为了方便后文叙述, 本文将 $SD_{i,j}(t_n)$ 简写为 $SD_{i,j}$ 。

4.2.3 卫星网络间接信任模型

在 LEO 卫星通信系统中,若卫星节点 i 对于邻居转发卫星节点 j 的直接信任不够充分时,此时就需将间接信任纳入信任评估的考虑因素中,既而求得卫星节点 i 对于邻居转发卫星节点 j 的聚合信任,以此来最终判定节点 j 是否可信。

在本文中,采用将距离卫星节点 j 一跳的第三方其他卫星节点对卫星节点 j 的直接信任值作为推荐信任值推荐给卫星节点 i 。同时,考虑到 LEO 卫星网络拓扑结构的特殊性与确定性,即每颗卫星有且最多只有 4 颗邻居节点卫星。因此,可利用这种特定的网络结构,来实现对推荐信任值的低开销、高效获取。首先,某一距离卫星节点 j 一跳的第三方其他卫星节点在计算完成对邻居转发卫星节点 j 的直接信任值后,只将不确定性 $m(\{T, \sim T\})$ 小于 1 的直接信任向量作为推荐信任值采取冗余发送。同时,限定最大转发跳数为 2 跳的方式进行传递。简单来讲就是说,推荐信任值首先会被发送给被评估卫星节点 j , 然后被评估卫星节点 j 再经过一跳发送至与其相邻的所有其他卫星节点 (包括卫星节点 i), 这样卫星节点 i 就可在较短时间内获取到第三方其他卫星节点的推荐信任值,并对推荐信任值进行相应的存储,以便后续在进行聚合信任计算,需要推荐信任值时,直接调用即可。优于像在地面移动 ad hoc 网络中通过广播质询请求包^[50],找到推荐节点后,再回复推荐信任值,来实现推荐信任值获取的形式。地面这种通过全网广播、无序获取推荐信任值的方式,会造成对链路带宽较多的浪费,且等待回复时间较长。不适合在 LEO 卫星网络这种特殊的、链路传播时延较长的网络中使用。具体 LEO 卫星节点获取其他节点推荐信任值的方式,如图 4-4 所示。

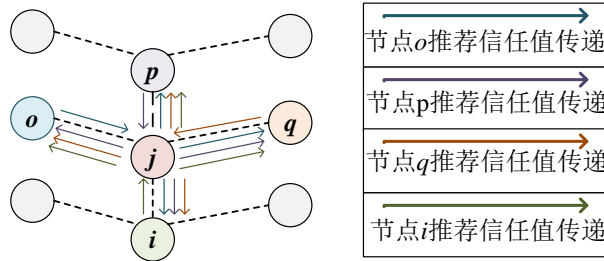


图 4-4 推荐信任值获取流程示意

但在推荐过程中,恶意卫星节点可能会发动诽谤攻击,提供虚假信任值。虚假信任值与其他信任值之间的证据冲突会造成信任合成与直觉相悖,导致非正常结果^[51]。折扣因子 $discount=[d_1, d_2, \dots, d_k]$ 的提出,则能够有效解决该问题^[52]。

卫星节点 i 对邻居转发卫星节点 j 的间接信任值设计成 $SI_{i,j}$ 。假如卫星节点 i 从 k 个不同距离卫星节点 j 一跳的第三方其他卫星节点 n_1, n_2, \dots, n_k 处收到了 k 个与卫星节点 j 相关的推荐信任向量为 $SI_{n_1,j}=(m_{n_1,j}(\{T\}), m_{n_1,j}(\{\sim T\}), m_{n_1,j}(\{T, \sim T\})), \dots,$

$SI_{nk,j} = (m_{nk,j}(\{T\}), m_{nk,j}(\{\sim T\}), m_{nk,j}(\{T, \sim T\}))$ 。接下来, 卫星节点 i 就可以采用证据距离^[47]公式, 推导出在这 k 个推荐信任向量当中, 任意 2 个不同推荐信任向量 p 和 q 之间的证据距离 $z_{p,q}$ 。 $z_{p,q}$ 代表的是第 p_{rank} 和第 q_{rank} 两个不同推荐信任向量之间的冲突剧烈情况。 $r_{p,q}$ 代表的是 p 与 q 二者之间的相似程度。故 $r_{p,q} = 1 - z_{p,q}$, $r_{p,q} = r_{q,p}$ 。至此, 全部 $r_{p,q}$ 可组成一个关于推荐信任向量的相似度矩阵 R 。

$$R = \begin{bmatrix} 1 & r_{1,2} & \cdots & r_{1,k} \\ r_{2,1} & 1 & \cdots & r_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ r_{k,1} & r_{k,2} & \cdots & 1 \end{bmatrix}_{k \times k} \quad (4-10)$$

根据 D-S 证据理论可知。当证据发生冲突时候, 若一个证据与其他大部分证据保持一定程度上的一致性时。那么, 此证据就应该被赋予较大权重, 强化这个证据对最终融合结果的益处; 相反, 若一个证据与其他大部分证据都不一致时。那么, 此证据就应该被赋予较小权重, 弱化这个突兀证据对最终融合结果的扰乱与破坏。所以, 在求得如公式(4-10)所示推荐信任向量的相似度矩阵后, 采用矩阵分析的手段, 来对每个卫星节点的推荐信任向量赋予不同的权重^[53]。

首先, 定义对第 p_{rank} 个推荐信任向量的支持度为 δ_p , 如公式(4-11)所示:

$$\delta_p = \sum_{q=1, q \neq p}^k R_{p,q} \quad (4-11)$$

然后, 标准权重 λ_p 被定义为公式(4-12)所示。

$$\lambda_p = \frac{\delta_p}{\sum_{q=1}^k \delta_q}, \text{ 且 } \sum_{p=1}^k \lambda_p = 1 \quad (4-12)$$

接下来, 选定标准权重因子中最大的因子 λ_{max} 作为关键证据, 既而获得每个推荐信任向量的折扣因子 $discount$, 如公式(4-13)所示:

$$discount = [d_1, d_2, \dots, d_k] = \frac{[\lambda_1, \lambda_2, \dots, \lambda_k]}{\lambda_{max}} \quad (4-13)$$

最终, 卫星节点 i 采用 $discount$ 对推荐信任向量做修正处理如公式(4-14)所示:

$$\begin{cases} m'_{i,j}(A) = ((m'_{n_1,j}(A) \oplus m'_{n_2,j}(A)) \oplus \cdots) \oplus m'_{n_k,j}(A) \\ m'_{n_l,j}(A) = d_l \times m_{n_l,j}(A), A \subset \Omega, l = 1, 2, \dots, k \\ m'_{n_l,j}(\Omega) = 1 - d_l + d_l \times m_{n_l,j}(\Omega) = 1 - \sum m'_{n_l,j}(A) \end{cases} \quad (4-14)$$

同时，由公式(4-14)可进一步求得修正后的卫星节点 i 对于卫星节点 j 的间接信任值，记为 $SI'_{ij}=(m_{ij}'(\{T\}), m_{ij}'(\{\sim T\}), m_{ij}'(\{T, \sim T\}))$ 。由上述可知，若一向量与其他向量冲突越剧烈，则其 *discount* 就越小，对最终信任合成破坏就越小。减小恶意卫星节点所带来的破坏，增强 LEO 卫星网络的可靠性与安全性。

4.2.4 卫星网络聚合信任模型

通过上述卫星网络的直接信任与间接信任模型的处理，便可得到修正处理后的直接信任 SD'_{ij} 与间接信任 SI'_{ij} 。然后卫星节点 i 采用 Dempster 合成法则对 SD'_{ij} 和 SI'_{ij} 进行合成，最终求得卫星节点 i 对邻居转发卫星节点 j 的聚合信任值 SC_{ij} ，即 $SC_{ij}=(m_{ij}^*(\{T\}), m_{ij}^*(\{\sim T\}), m_{ij}^*(\{T, \sim T\}))$ ，满足如公式(4-15)所示约束：

$$\begin{cases} m_{i,j}^*(A) = ((m_{n_1,j}'(A) \oplus m_{n_2,j}'(A)) \oplus \dots) \\ \quad \oplus m_{n_k,j}'(A) \oplus m_{i,j}'(A), A \subset \Omega \\ m_{i,j}^*(\emptyset) = 0 \end{cases} \quad (4-15)$$

若节点 j 与其全部邻居转发卫星节点皆无交互历史，此时是获取不到对卫星节点 j 的间接信任值。因此，此时就把卫星节点 i 对邻居转发卫星节点 j 的修正直接信任 SD'_{ij} ，当成节点 i 对节点 j 的聚合信任 SC_{ij} 。

4.3 算法设计

本节主要介绍 SLT 算法的设计基本思想，以及 SLT 运行过程中涉及的 3 个相辅相成模块：基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块。

4.3.1 基本思想

采用信任管理安全加固的理念，进行信任路由设计时。首先，都需提出一种合理、有效的信任评估模型。其次，将信任评估模型与原料路由协议相融合改造。最终，就可以得到一种新型的基于节点信任度的安全路由算法。目前，应用于卫星网络的信任路由方案多是以下两种形式：

(1) 将地面网络中的信任路由方案改造迁移至卫星网络。此类信任路由方案多是以地面传统移动 ad hoc 网络路由协议（如 DSR、AODV 等），作为原料路由协议，然后与信任评估模型相融合得到的卫星网络信任路由方案^[54]。虽然 LEO 卫星网络是一种特殊的、具有规律运动特点的空间移动 ad hoc 网络。但是，直接采用地面移动 ad hoc 网络的路由协议，作为信任改造所使用的原料路由协议的话，对于解决卫星网络内部路由攻击问题不具有针对性与特定性。例如以 AODV 协议

作为原料路由协议，进行信任改造所得到的安全路由。其在实际运行寻找可行路径的时候，会在卫星全网范围内洪泛 RREQ 路由请求包，极大地消耗了卫星网络有限的带宽资源。且星间链路传播时延也较长，拓扑变化也较为剧烈。因此，RREP 所回复的路由转发路径也可能已过时、失效，不能较好地适应卫星网络的内在运动特点，也就大大降低了此类信任路由所带来的有益安全防护效果。

(2) 采用跨层卫星协作的方式实现信任安全路由。如采用 MEO 卫星与 LEO 卫星相配合的方式^[55-56]。首先，MEO 卫星对 LEO 卫星实施分组管理。同时，设定 MEO 卫星只具有路由管理功能且假定为绝对可信的，LEO 卫星节点只负责数据的路由转发。然后，MEO 卫星负责收集和统计 LEO 卫星节点的路由行为，并结合相应信任评估模型，识别和隔离恶意 LEO 卫星节点，完成相应安全式路由表的计算与下发。最后，LEO 卫星节点就可依据路由表实现数据的安全传输。但此方案实现难度较大，MEO 卫星与 LEO 卫星之间的相对运动剧烈，卫星间协作难度较大，且假设 MEO 卫星为绝对可信也不太合理，故此方案也不可取。

基于以上两种方案分析，针对 LEO 卫星网络这种特殊分布式网络系统，急需设计一种特定、合理的动态信任路由方案，用以防护内部路由攻击行为。因此，本文在综合考虑了 LEO 卫星网络的内在运动特点以及在 LEO 卫星网络中实施信任管理的特殊性。决定将一种基于轨道预测的低开销 LEO 卫星路由协议 OPSPF 作为原料路由协议，进行信任安全加固改造。OPSPF 路由协议是假设系统运行于安全环境中的，网络中的每颗卫星也都是绝对可信，并没有针对路由攻击提供可靠的安全防护措施。一旦网络中存在恶意节点并发起如黑洞、灰洞等攻击行为，就会造成较为严重的网络故障，甚至系统瘫痪。因此，本文将 OPSPF 作为原料路由协议，并融合本文所提出的基于 D-S 证据理论的 LEO 卫星网络信任评估模型，进行安全信任加固改造，设计实现 SLT 安全路由算法。

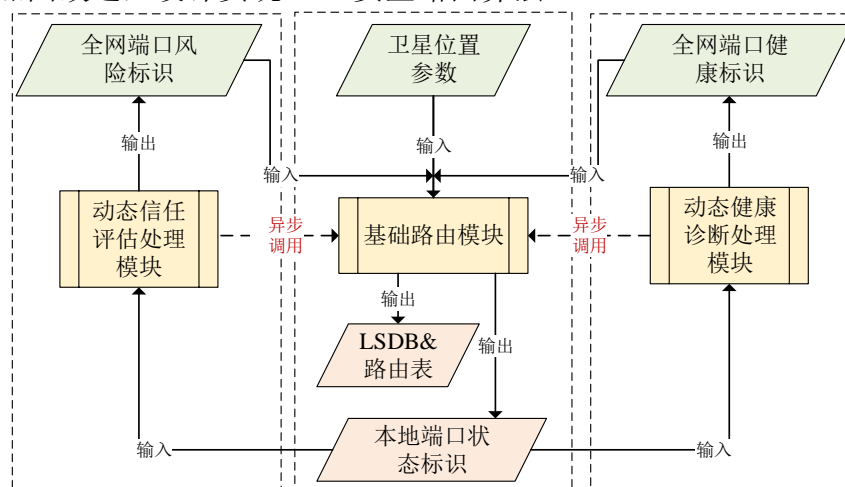


图 4-5 SLT 算法整体设计框架

SLT 算法的运行，主要由三个功能模块间的相辅相成实现，包括：基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块，如图 4-5 所示。

首先，对 SLT 算法各组成部分作简要介绍：

(1) **基础路由模块**：SLT 算法核心组成部分，通过输入卫星位置信息、全网端口风险标识以及全网端口健康标识等参数参与运算。既处理 LEO 卫星网络中的规律性事件（规律性拓扑变化），亦同时融合处理非规律事件（动态信任评估处理模块提供恶意卫星节点信息、动态健康诊断处理模块提供非规律拓扑变化信息），实现对链路状态数据库（Link State Data Base, LSDB）、路由表以及本地端口状态标识的更新。此模块由卫星节点同步周期性调用（实现路由表周期性更新）与由动态信任评估处理模块与动态健康诊断处理模块异步触发调用（实现路由表触发式更新）。维护得到安全式无失效无故障链路路由表，用以指导数据包转发。

(2) **动态信任评估处理模块**：通过基于 D-S 证据理论的 LEO 卫星网络信任评估模型，对 LEO 卫星网络中的每颗卫星实施周期性分布式动态信任评估。及时检测并处置恶意卫星节点，实现对全网端口风险标识的更新。并异步调用基础路由模块，实现对恶意卫星节点的隔离，防止恶意卫星节点加入路由转发路径。

(3) **动态健康诊断处理模块**：通过 Hello 报文的动态探测，实现对 ISL 的周期性检测，及时捕获发现 LEO 卫星网络的不规律拓扑变化，如突发性 ISL 故障、故障 ISL 恢复等。实现对全网端口健康标识的更新，并异步调用基础路由模块，实现发生 ISL 故障或故障 ISL 恢复时的路由重构。

然后，对 SLT 算法运行过程中所涉及各类表与标识进行简要介绍。包括存储位置、更新执行者以及更新时刻，如下表 4-1 所示。

表 4-1 表结构及标识

名称	存储位置	更新执行者	更新时刻
LSDB	卫星	基础路由模块	执行基础路由模块时
路由表	卫星	基础路由模块	执行基础路由模块时
全网端口风险标识	卫星	动态信任评估处理模块	判定邻居节点为恶意节点时；收到与本地不相同的风险通知 LSU 报文
全网端口健康标识	卫星	动态健康诊断处理模块	判定邻居端口故障或恢复时；收到与本地不相同的健康通知 LSU 报文
本地端口状态标识	端口	基础路由模块	执行基础路由模块时
链路保活计数器	端口	动态健康诊断处理模块	发送出 Hello 报文时；接收到 Hello 报文时；本地故障端口恢复时

其中，LEO 卫星执行基础路由模块情况：

(1) 基础路由模块的同步周期性执行。

(2) 动态信任评估处理模块与动态健康诊断处理模块的异步触发调用，包括：判定邻居节点为恶意节点、收到与本地不相同的风险通知 LSU 报文、判定邻居端口故障或恢复时、收到与本地不相同的健康通知 LSU 报文、本地故障端口恢复时。

当检测出恶意节点或故障发生与故障恢复时，均需要通过洪泛 LSU 包的形式向全网通告恶意卫星节点或 ISL 异常信息，实现卫星全局拓扑同步。由于恶意节点或突发性 ISL 异常为小概率发生事件。因此，由全网洪泛 LSU 带来的开销较小，对带宽占用较少。因此，不会对网络的性能造成太大的影响。

最后，对 SLT 算法中所涉及各类标识作简要定义，卫星的每个端口全都具有三种不同标识，用以处理不同事件。其中，包括全网端口风险标识、全网端口健康标识以及本地端口状态标识，如下图 4-6 所示。

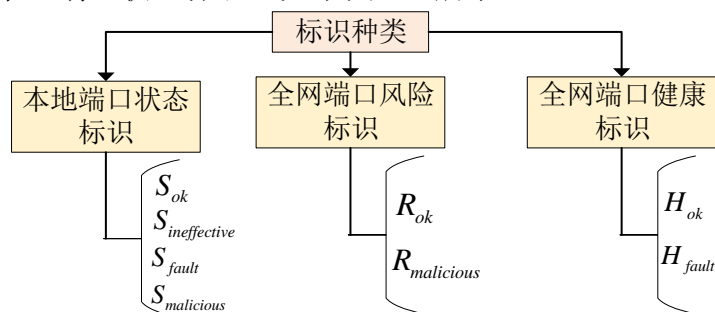


图 4-6 标识分类

(1) 设置全网端口风险标识的目的，是为了对全网每个恶意端口在 LSDB 中所对应链路的删除修正，由每颗卫星在本地维护。当某颗卫星被判定为恶意节点时，其所有端口都会被认为是危险的。因此，将其对应端口的风险标识修改为恶意，即定义为 $R_{malicious}$ ，该端口对应的链路也会在 LSDB 中被删除；当卫星节点为正常节点时，端口风险标识为正常，即定义为 R_{ok} ，此时该端口对应的链路则会在 LSDB 中继续保留。

(2) 设置全网端口健康标识的目的，是为了对全网每个故障端口在 LSDB 中所对应链路的删除修正，由每颗卫星在本地维护。当某个卫星端口发生故障时，则该故障端口的健康标识被修改为故障，即定义为 H_{fault} 。此时该端口对应的链路会在 LSDB 中被删除；当卫星端口正常工作时，其端口对应的健康标识为正常，即定义为 H_{ok} ，此时该端口对应的链路则会在 LSDB 中继续保留。

(3) 设置本地端口状态标识的目的，是为了卫星在本地判定自身四个端口是否可通信，是动态信任评估处理模块与动态健康诊断处理模块运行前提。只有为

可通信端口时,即本地端口为非失效、非恶意、非故障状态时,则此本地端口的状态标识定义为 S_{ok} ,卫星才可以从该正常端口发送与接收 Hello 报文,转发与接收 LSU 报文;其余情况皆为不可通信端口:①位于极圈内或反向缝位置时,异轨道间链路断开(失效链路),若断链路为某颗卫星的某一端口所具有的,则该卫星对应本地端口的状态标识修改为 $S_{ineffective}$;②当某颗卫星判定或通过接收风险通知 LSU 报文得知其邻居卫星为恶意卫星节点时,此时,该卫星与恶意卫星建立链路的那个本地端口的状态标识会被修改为 $S_{malicious}$;③当卫星发现其邻居卫星端口故障时,该卫星与故障卫星建立链路的那个本地端口的状态标识会被定义为 S_{fault} ,或当故障卫星接收到关于自身某个端口为故障的健康通知 LSU 报文时,故障卫星也会将对应本地故障端口的状态标识修改为 S_{fault} ;另外,设定不可通信本地端口对应的状态标识应具有优先级,为 $S_{ineffective} > S_{malicious} > S_{fault}$,当卫星的某个本地端口具有 2 个及以上不可通信事件发生时,取优先级最高的状态标识代表此时本地端口的状态标识。

4.3.2 基础路由模块

SLT 算法的核心组成部分基础路由模块,如图 4-7 所示:处理 LEO 卫星网络中的规律性事件(规律性拓扑变化,如极圈内与反向缝位置时异轨道间 ISL 断开);同时,融合处理非规律事件(动态信任评估处理模块提供恶意卫星节点信息、动态健康诊断处理模块提供非规律拓扑变化信息)。

首先,由于非规律事件的发生概率极小。因此,原先 LEO 卫星网络中的拓扑同步开销主要是由规律性事件引起的。因此,本文基础路由模块继承了 OPSPF^[39] 协议中通过轨道预测推导全局卫星位置,并根据卫星位置与运动方向因素得到初步 LSDB 的设计理念。直接将原来由规律性拓扑变化所引起的拓扑同步收敛开销降为 0。由于本文处理规律性拓扑变化所实现的拓扑同步是通过本地推导算法实现,而不是通过全网路由信息动态交互收敛得来的(收敛时间与网络延迟无关)。因此,基础路由模块的执行周期可设定比较小,以适应高动态拓扑变化。

然后,在得到初步 LSDB 后,接下来对卫星网络中的非规律事件进行处理。通过遍历由动态信任评估处理模块和动态健康诊断处理模块所提供的全网端口风险标识和全网端口健康标识,删除恶意端口和故障端口所对应的链路,得到全面修正后的 LSDB。

最终,可得到一个无失效、无恶意以及无故障链路的 LSDB,运行最短路径算法,既而完成安全式路由表项更新。同时,根据卫星位置信息、运动方向、端口风险标识以及端口健康标识来实现本地端口状态标识的更新。

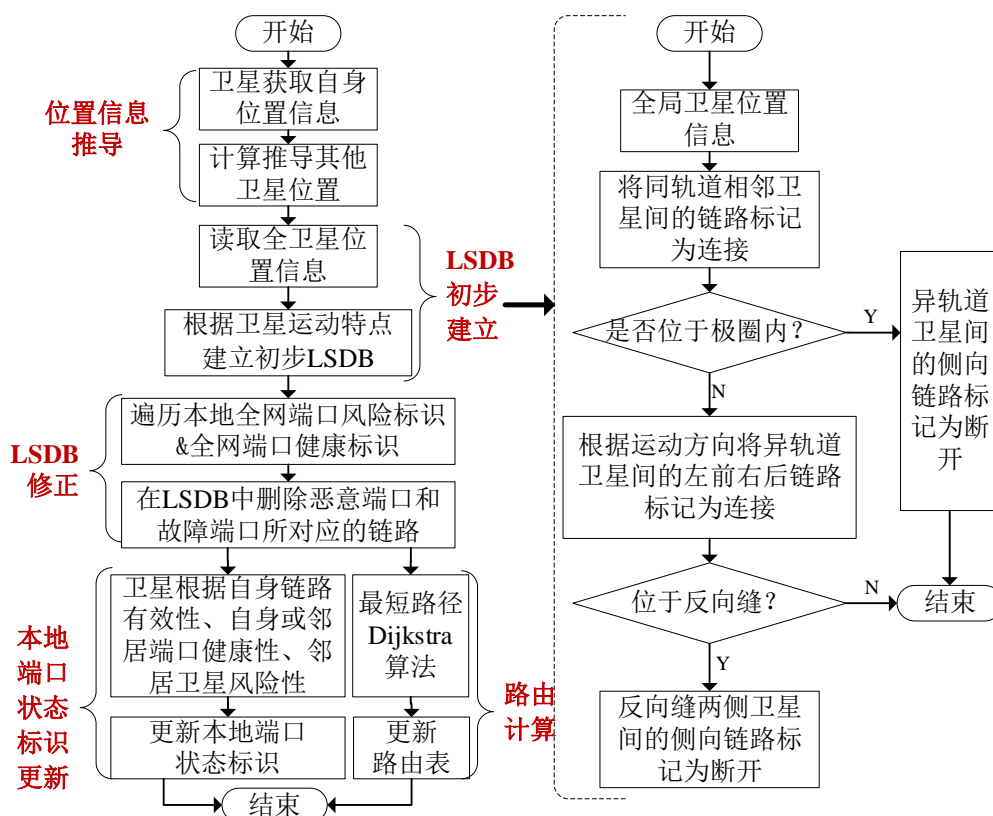


图 4-7 基础路由模块运行流程

因此，将此模块分为 5 阶段介绍：位置信息推导阶段、LSDB 初步建立阶段、LSDB 修正阶段、路由计算阶段以及本地端口状态标识更新阶段。

4.3.2.1 位置信息推导阶段

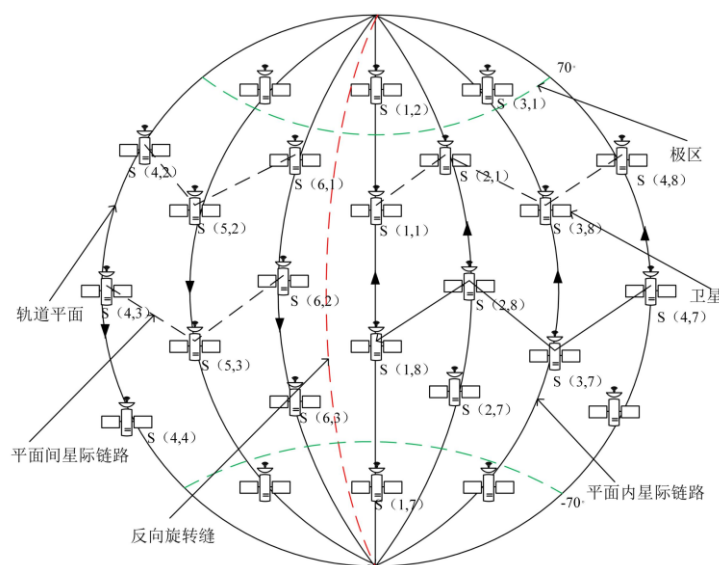


图 4-8 LEO48 星座网络

在位置信息推导阶段，主要目的是为完成全局卫星位置信息推导。推导出全局卫星位置信息后，此阶段认为每颗卫星与其周围所有邻居转发卫星全联通，即全网络可通达。后续阶段再去修正此阶段假设所得的卫星网络全联通拓扑图。

此阶段，LEO 卫星会根据自身位置信息以及卫星运动规律，推导出其他卫星位置。本章以 LEO48 星座作为安全路由算法设计背景，此星座中共有 48 颗卫星，分布在 6 个轨道面上，单轨面上各有 8 颗卫星，如图 4-8 所示。且定义 $S(\alpha, \beta)$ 为每颗卫星的编址描述， α 代表轨道面号， β 代表此轨道面上本颗卫星编号。如 $S(1, 1)$ 代表的是第 1 轨道面上，编号为 1 的卫星。星座式卫星网络运动具有以下特点：

(1) 位于同轨道面上的卫星，具有相同的经度坐标，8 颗卫星均匀分布在同一轨道面上。因此，轨内相邻卫星间的相位差为 45° 。

(2) 对于异轨道卫星。星座中的 6 个轨道面均匀分布。故相邻轨道卫星的经度差为 30° 。由公式(4-16)可知，卫星轨道高度 h 决定了卫星的运动周期 T 。因为，各卫星的 h 一样。所以，不同轨道的卫星 T 也一样。

$$T = 2\pi \sqrt{\frac{(r_e + h)^3}{\mu}} \quad (4-16)$$

根据星座式卫星网络中卫星运动特点。首先，根据卫星自身的位置信息推导出同轨道上其他全部卫星的位置信息。其次，又因为相邻轨道的相位差是一个定值。因此，可推导出相邻轨道相同编号卫星的位置信息。然后，再利用同轨道卫星位置信息推导方法，求得相邻轨道面上的全部卫星位置信息。最终，可逐步求得 LEO48 星座的全部 48 颗卫星的位置信息。根据此卫星位置信息推导思想，提出了此阶段的卫星位置信息推导算法，具体的伪代码实现如下表 4-2 所示。

表 4-2 位置信息推导算法

算法 4-1：位置信息推导算法：

*/*参数定义*/*

M//轨道面数

N//单轨道面上卫星颗数

$S(\alpha, \beta)$ //其中， α 代表轨道编号， β 代表此轨道上本颗卫星编号

$S(\alpha, \beta).lon$ // $S(\alpha, \beta)$ 的经度，经度范围 $[-180, 180]$

$S(\alpha, \beta).lat$ // $S(\alpha, \beta)$ 的纬度，纬度范围 $[-90, 90]$

diff0//轨内相邻卫星相位差， $360/N$

diff1//相邻轨道同编号卫星相位差，一般是一个定值

diff2//相邻轨道卫星经度差， $180/M$

```

d//方向因子，卫星往北运动时，令  $d=1$ ；卫星往南运动时令  $d=-1$ 
flag//初值为 0，用作循环结束条件的判定
/*具体算法*/
1: for( $i=\alpha$ ;  $i=(i+1)\%M$ ){//遍历全部轨道
2:   if( $flag==1 \&\& i==\alpha \&\& j==\beta$ ) break;
3:   if( $i!=\alpha$ ){//计算相邻轨道同编号卫星位置信息
4:      $S(i, \beta).lon = (S((i+M-1)\%M, \beta).lon + diff2 + 180) \% 360 - 180$ ;//经度范围为 $[-180, 180]$ 
5:      $S(i, \beta).lat = S((i+M-1)\%M, \beta).lat + diff1 * d$ ;
6:     if( $S(i, \beta).lat > 90$ )  $S(i, j).lat = 180 - S(i, j).lat$ ;
7:     if( $S(i, \beta).lat < -90$ )  $S(i, j).lat = -180 - S(i, j).lat$ ;
8:   }
9:   for( $j=\beta$ ;  $j=(j+1)\%N$ ){//遍历同轨道卫星
10:    if( $i==\alpha \&\& j==\beta$ ) {
11:      if( $flag==0$ ) {
12:         $flag=1$ ;
13:        continue;//跳过当前卫星
14:      }
15:      else break;
16:    }
17:    //计算同轨道上其他卫星的位置信息
18:     $S(i, j).lon = S(i, (j+N-1)\%N).lon$ ;
19:     $S(i, j).lat = S(i, (j+N-1)\%N).lat + diff0 * d$ ;
20:    if( $S(i, j).lat > 90$ )  $S(i, j).lat = 180 - S(i, j).lat$ ;
21:    if( $S(i, j).lat < -90$ )  $S(i, j).lat = -180 - S(i, j).lat$ ;
22:  }
23:}

```

4.3.2.2 LSDB 初步建立阶段

LSDB 是路由表计算前提，所以 LEO 卫星网络中每颗卫星都会在本地图维护 LSDB，类同于地面内部网关协议 OSPF 的 LSDB。本文 LSDB 存储了全网可通信 ISL 信息。本文 LSDB 构建分为两阶段：LSDB 初步建立阶段以及 LSDB 修正阶段。

LSDB 初步建立阶段，主要处理卫星规律性事件（规律性拓扑变化，如在极圈内与反向缝位置时，异轨道间 ISL 断开）所造成的失效链路。此阶段考虑卫星所

处位置信息以及卫星运动方向，从而对位置信息推导阶段假设所得的卫星网络全联通拓扑图进行初步修正，修正流程如图 4-7 右侧所示。删除 70° 极圈内（卫星位置因素）以及反向缝位置时（运动方向因素）异轨 ISL。而其余像同轨以及异轨卫星间可通信 ISL 则继续保持。经此阶段处理，就可得到无失效链路 LSDB。

4.3.2.3 LSDB 修正阶段

LEO 卫星网络中除存在规律事件发生，还可能存在像恶意卫星节点以及卫星端口故障等特殊、非规律事件发生。故需对 LSDB 初步建立阶段所得 LSDB 做进一步修正。非规律事件包括：由动态信任评估处理模块提供恶意卫星节点信息和由动态健康诊断处理模块提供不规律拓扑变化信息（突发性 ISL 故障、故障恢复）。

首先，通过遍历本地存储的全网端口风险标识，在 LSDB 中删除端口风险标识为 $R_{malicious}$ 端口所对应链路，由于恶意卫星节点所有端口的端口风险标识都会被标记为 $R_{malicious}$ 。因此，恶意卫星节点所具有的全部链路都会被删除，实现了对恶意卫星节点的隔离。其次，通过遍历本地存储的全网端口健康标识，在 LSDB 中继续删除端口健康标识为 H_{fault} 端口所对应的链路。

最终，经 LSDB 初步建立以及 LSDB 修正两阶段处理，就可得到一个无失效、无故障链路以及无恶意节点对应链路的 LSDB。

4.3.2.4 路由计算阶段

在完成上述位置信息推导、LSDB 初步建立以及 LSDB 修正三阶段处理后。最终，每颗卫星就可得到一个无失效、无故障链路以及无恶意节点对应链路的 LSDB。

表 4-3 路由表结构

目的卫星节点地址	下一跳卫星节点地址	跳数
Dest_Satellite_ID ₁	Next_Satellite_ID ₁	Hop ₁
Dest_Satellite_ID ₂	Next_Satellite_ID ₂	Hop ₂
...
Dest_Satellite_ID _{num}	Next_Satellite_ID _{num}	Hop _{num}

接下来，卫星根据 LSDB，在其上运行 Dijkstra 最短路径算法，就可计算出自己到其他所有卫星节点的最短路径，使其更新的路由转发路径上不包含失效、故障链路以及恶意卫星节点。对 LEO 卫星网络路由协议实现了较为可靠的安全防护。既而完成路由表的更新。每颗卫星依照路由表的指导，就可完成对数据包的逐跳转发。具体的路由表项结构，如表 4-3 所示。

但是,使用 Dijkstra 最短路径算法进行计算时,需要在拓扑表中标注每条链路的代价。由于本文中 LSDB 的获得是通过推导而来,并没有对链路代价值(如带宽、时延等)进行收集。因此,在本文中统一将每条链路的代价值设定为 1,实际上就变成了计算最小跳数的路由。同时,由于本文采用 Dijkstra 算法完成最短路径的计算。因此,其时间复杂度为 $O(|V|^2)$ 。其中, V 代表卫星网络中卫星节点数量。

4.3.2.5 本地端口状态标识更新阶段

此部分关于本地端口状态标识更新实现,与 4.3.1 节基本思想中关于各类标识的定义中的本地端口状态标识介绍一致。因此,不做赘述。

4.3.3 动态信任评估处理模块

本节是对动态信任评估处理模块的描述,依据 4.2 节所提出的基于 D-S 证据理论的 LEO 卫星网络信任评估模型,对 LEO 卫星网络中的节点实施周期性地信任评估。但在检测识别出恶意卫星后,还需给出后续相应安全处理。因此,本节主要介绍对恶意卫星节点的处置以及风险通知 LSU 报文处理两部分内容。

4.3.3.1 恶意卫星节点处置

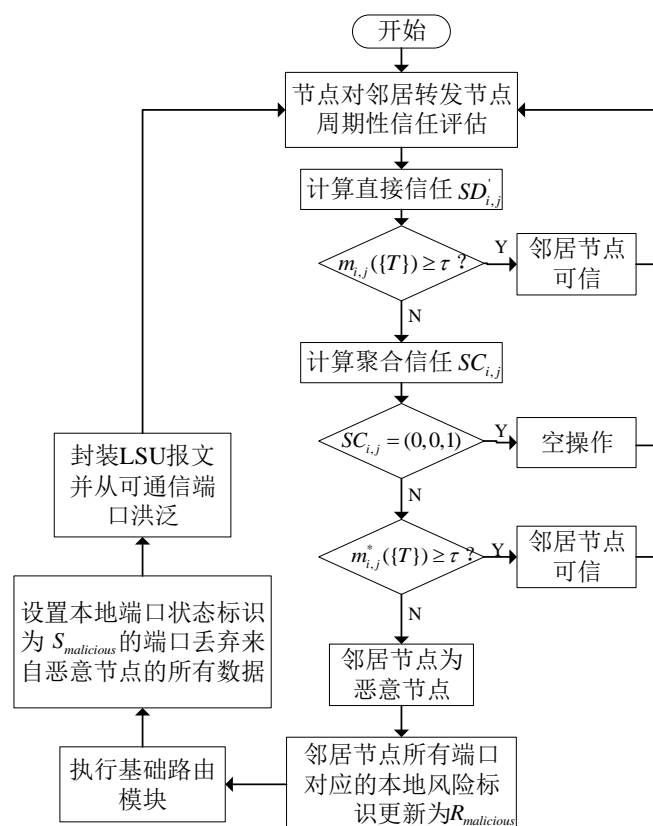


图 4-9 恶意卫星节点判定及其隔离处置流程

采用本章所提出的 LEO 卫星网络的动态信任评估模型,就可以对卫星节点的信任度实施准确的周期性信任评估,及时捕获卫星网络中的恶意卫星节点,并进行有效、迅速的隔离,最大化程度避免安全事件的发生。以上为具体的恶意卫星节点判定识别以及隔离处置流程示例,如图 4-9 所示。

在对 LEO 卫星网络进行信任评估,识别恶意卫星节点之前。首先,需要设定一个合理的安全判定阈值常量 $\tau(0.5 \leq \tau \leq 1)$ 。节点信任值低于阈值 τ 的卫星节点,则认为是恶意卫星节点。具体恶意卫星节点判定识别步骤如下所示:

(1) 卫星节点在对其邻居转发卫星节点周期性信任评估后。首先,采用直接信任向量的 $m_{ij}(\{T\})$ 与阈值 τ 进行比较。若 $m_{ij}(\{T\}) \geq \tau$, 则认为邻居转发卫星节点可信;否则,转至步骤(2)。

(2) 在直接信任不充分时。此时,就需要将间接信任纳入进来,计算聚合信任,来对邻居转发卫星节点,作进一步信任与否的判定。若聚合信任向量 $SC_{ij}=(0, 0, 1)$ 时。那么,就说明对于邻居节点不确定性为 1。因此,不做任何处理;否则,转至步骤(3)。

(3) 将聚合信任向量的 $m_{ij}^*(\{T\})$ 与阈值 τ 进行比较,若 $m_{ij}^*(\{T\}) \geq \tau$, 则认为邻居转发卫星节点可信;否则,则认为邻居转发节点为恶意卫星节点。

若邻居转发卫星节点被判定为是一颗恶意卫星节点后。接下来,就需将此恶意卫星节点采取有效隔离防护。在 LSDB 中删除该恶意邻居转发卫星节点所对应的全部链路,得到一张安全的卫星网络拓扑。并在拓扑上运行最短路径 Dijkstra 算法,就可以得到安全、可信没有恶意卫星节点参与的路由转发路径,实现安全式路由计算。具体恶意卫星节点隔离处置步骤如下所示:

(1) 把邻居转发卫星节点的所有端口,在本地全网端口风险标识中的对应项更新为 $R_{malicious}$ 。

(2) 执行基础路由模块,用来更新本地端口状态标识、LSDB 和路由表。

(3) 设置本地端口状态标识为 $S_{malicious}$ 端口丢弃来自恶意节点的所有数据。

(4) 将邻居转发卫星节点是恶意卫星节点的信息,封装成风险通知 LSU 报文,并在可通信端口间洪泛。

4.3.3.2 风险通知 LSU 报文处理

如图 4-10 所示,展示了风险通知 LSU 报文的处理流程。LEO 卫星节点从可通信端口收到 LSU 报文后。首先,会判别该报文是否为风险通知 LSU 报文。若不是,则交由健康通知 LSU 报文处理机制处理;否则,就把此风险通知 LSU 报文信息与本地全网端口风险标识进行对比,判定是否相同。

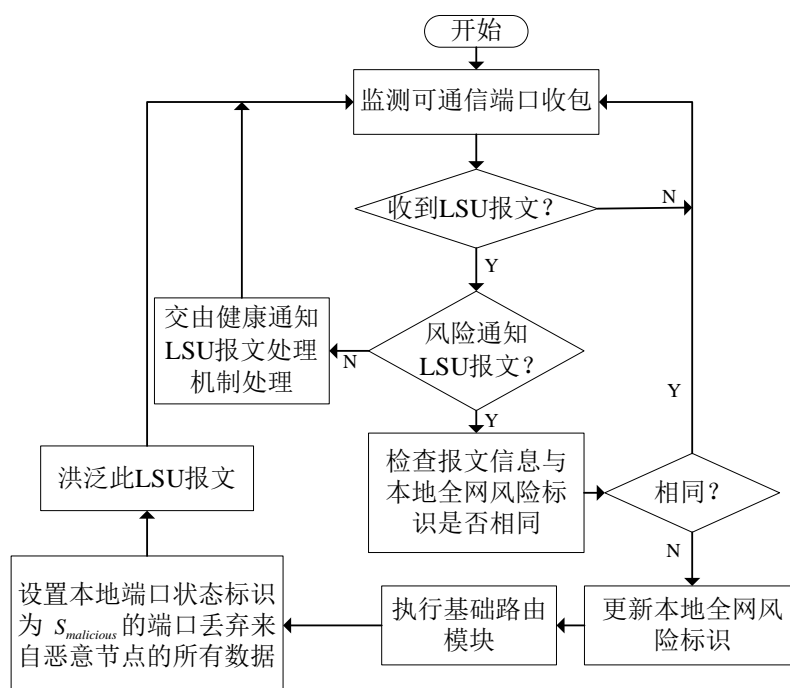


图 4-10 风险通知 LSU 报文处理流程

具体对比判定方式，如表 4-4 所示。

表 4-4 风险通知 LSU 报文信息与对应本地全网端口风险标识情况

风险通知 LSU 报文信息	本地全网端口风险标识
恶意卫星节点	报文中目的恶意卫星所有端口标识为 $R_{malicious}$

如果风险通知 LSU 报文信息与本地全网端口风险标识对比后，发现相同。那么，就不需要处理（要求每颗卫星只会把每条风险通知 LSU 报文信息处理 1 次）。否则，就开展如下操作：

- （1）把本地全网端口风险标识更新为，与风险通知 LSU 报文相同。
- （2）执行基础路由模块，用来更新本地端口状态标识、LSDB 和路由表。
- （3）设置本地端口状态标识为 $S_{malicious}$ 的端口丢弃来自恶意节点的所有数据。
- （4）继续在可通信端口间洪泛此风险通知 LSU 报文。

4.3.4 动态健康诊断处理模块

在 LEO 卫星通信系统实际运行过程中，还可能会存在不规律事件的发生。如卫星设备异常所造成的突发性 ISL 故障，会造成传输数据的被迫丢失，降低路由转发可靠性。

因此，在路由算法设计时。不仅要考虑像在极圈内、反向缝位置时造成异轨

道间 ISL 断开（极轨道星座内在运动特点考虑），实时检测与隔离恶意节点（路由安全性考虑）。还应使路由算法具有动态链路故障检测的能力（设备运行可靠性考虑），使之及时更新路由路径，避开故障链路，降低数据丢包的损失。

本节是对动态健康诊断处理模块的介绍，主要分为动态检测链路故障发生、动态检测故障链路恢复以及健康通知 LSU 报文处理三部分，下面将展开详细描述。

4.3.4.1 动态检测链路故障发生与处置

动态检测链路故障的发生与处置流程如图 4-11 所示。每颗 LEO 卫星会为每个星间端口，维护 1 个 ISL 保活计数器 Counter。卫星会周期性地从每个可通信端口往外发送 Hello 报文，用来探测对应 ISL。每当发送 1 次 Hello 报文，则该端口的 Counter 值会做减 1 处理。若 Counter 值减到为 0 时，那么就认为 ISL 保活超时。Counter 初值与 Hello 报文发送间隔相乘得到 ISL 保活期。如果在 ISL 保活期内，可通信端口收到了 Hello 报文，那么就将此端口所对应的 Counter 值重置；如果在 ISL 保活期内并没有收到 Hello 报文，此时就认为邻居端口故障。开展如下操作：

- （1）把邻居端口在本地全网端口健康标识中的对应项更新为 H_{fault} 。
- （2）执行基础路由模块，用来更新本地端口状态标识、LSDB 和路由表。
- （3）把 ISL 故障信息封装成健康通知 LSU 报文，并在可通信端口间洪泛。

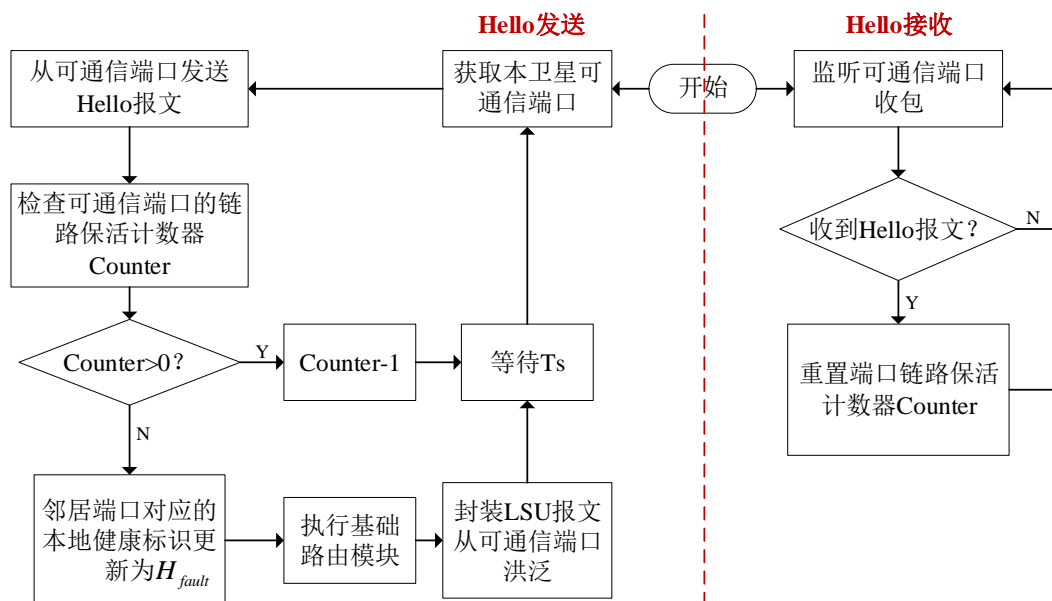


图 4-11 动态检测链路故障发生与处置流程

4.3.4.2 动态检测链路故障恢复与处置

因本文使用了健康标识标记 ISL 故障。但在 ISL 故障恢复时，此标识仍旧存在。因此需对 ISL 故障恢复，进行相应动态检测与处置。具体流程如图 4-12 所示。

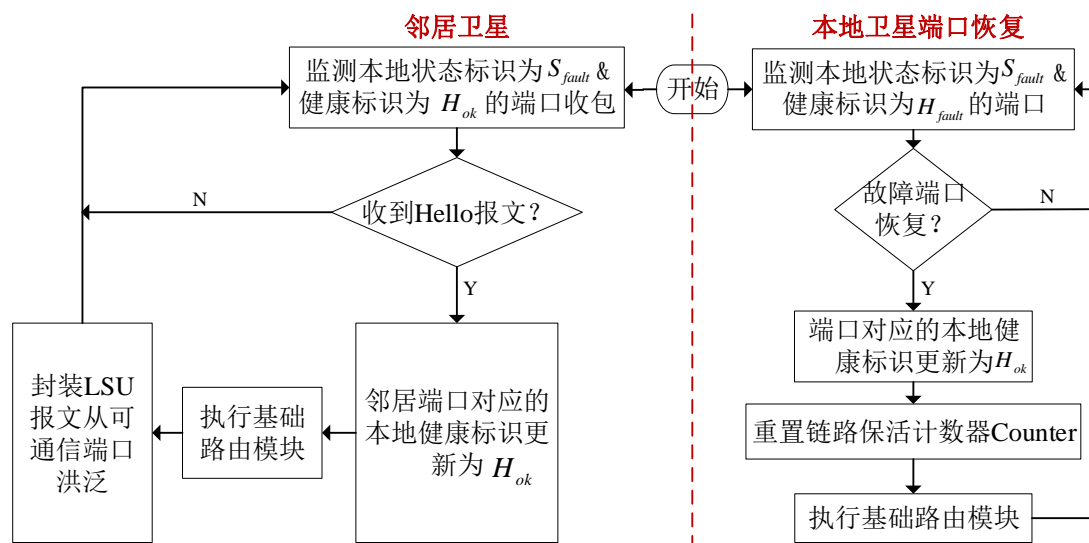


图 4-12 动态检测链路故障恢复与处置流程

将故障端口分为本地故障端口与邻居故障端口。当动态检测到本地故障端口（即监测到本地状态标识为 S_{fault} & 端口健康标识为 H_{fault} 的端口）恢复后，进行如下操作：

- （1）把此端口在本地全网端口健康标识中的对应项更新为 H_{ok} 。
- （2）重置此端口对应的 Counter 值。
- （3）执行基础路由模块，用来更新本地端口状态标识、LSDB 和路由表。

对于本地故障端口的恢复情况，卫星是不需向全网进行通告。而是由邻居卫星进行发现并完成通告的。每颗卫星从基础路由模块所标记的可通信端口，周期性发送 Hello 报文。如果动态健康诊断处理模块所标记的故障端口（即监测到本地状态标识为 S_{fault} & 端口健康标识为 H_{ok} 的端口）收到 Hello 报文时，则认为邻居端口故障已恢复。接下来，对此端口进行如下操作：

- （1）把邻居端口在本地全网端口健康标识中的对应项更新为 H_{ok} 。
- （2）重置此端口对应的 Counter 值。
- （3）执行基础路由模块，用来更新本地端口状态标识、LSDB 和路由表。
- （4）把 ISL 故障恢复信息封装成健康通知 LSU 报文，并在可通信端口间洪泛。

4.3.4.3 健康通知 LSU 报文处理

如图 4-13 所示，展示了健康通知 LSU 报文处理流程。LEO 卫星从可通信端口收到 LSU 报文后。首先，会判别该报文是否为健康通知 LSU 报文。若不是，则交由风险通知 LSU 报文处理机制处理；否则，就把此健康通知 LSU 报文信息与本地全网端口健康标识进行对比，判定是否相同。

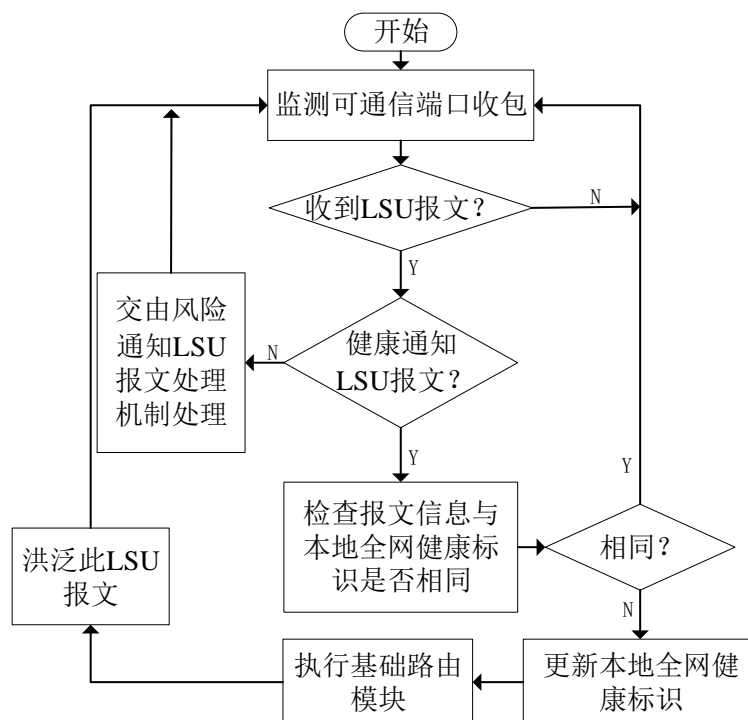


图 4-13 健康通知 LSU 报文处理流程

具体的对比判定方式，如表 4-5 所示。

表 4-5 健康通知 LSU 报文信息与对应本地全网端口健康标识情况

健康通知 LSU 报文信息	本地全网端口健康标识
ISL 故障	报文中目的卫星目的端口标识为 H_{fault}
ISL 故障恢复	报文中 2 个端口在标识中的对应项均是 H_{ok}

如果健康通知 LSU 报文信息与本地全网端口健康标识对比后，发现相同。那么，就不需要处理（要求每颗卫星只会把每条健康通知 LSU 报文信息处理 1 次）。否则，就开展如下操作：

- （1）把本地全网端口健康标识更新为，与健康通知 LSU 报文相同。
- （2）执行基础路由模块，用来更新本地端口状态标识、LSDB 和路由表。
- （3）继续在可通信端口间洪泛此健康通知 LSU 报文。

4.4 仿真设计及结果分析

本节将采用 NS2^[37-38]网络仿真软件，来完成对本文所提出的 SLT 路由算法与文献[44]提出的基于轨道预测 OPSPF 路由算法之间，在分组投递率、丢包率以及平均端到端时延等安全性能方面的对比仿真。

4.4.1 仿真环境和参数设置

由于 STK^[39] 卫星仿真软件不支持卫星网络路由算法的仿真。而 OPNET^[40] 网络仿真软件的使用成本较高。且对其网络底层构件的修改，也较为困难。因此，本文决定使用免费开源的、面向对象基于离散事件驱动的 NS2 网络仿真软件，来完成对各 LEO 卫星网络路由算法的仿真测试。NS2 目前支持极轨道卫星星座的仿真实现，且 NS2 是采用 2 种面向对象的语言来完成开发实现：C++ 与 OTcl。本文是在 NS2 所提供的卫星网络仿真基础之上，修改了部分代码，来完成实现各卫星网络路由算法：SLT 路由算法与 OPSPF 路由算法。通常 NS2 的网络仿真流程，如图 4-14 所示。

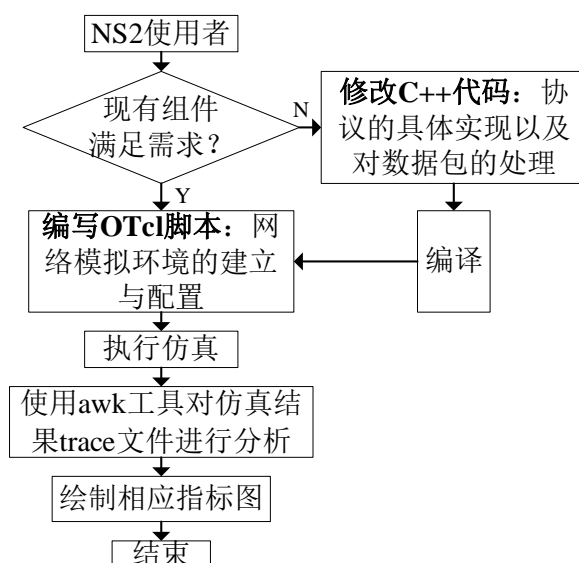


图 4-14 NS2 网络仿真流程

采用 NS2 进行网络仿真时，需要对各仿真参数进行详细设定。

首先，关于地面用户终端选择接入卫星的方式。设定地面用户终端根据最长覆盖时间的原则，来决定接入卫星。同时，设定地面用户终端每隔 10s，对其服务卫星的最小仰角进行检查。若不满足，则及时进行接入卫星的切换。

表 4-6 地面用户终端仿真参数

核心参数	数值
仿真时间 (s)	100
数据流类型	CBR
终端发送速率 (packet/s)	30
数据包大小 (Bytes)	1000

其次, 设定地面终端产生 CBR 类型的数据流, 具体参数如表 4-6 所示。同时, 为了模拟出 LEO48 星座网络中真实的流量分布情况。因此, 通过基于人口密度因素, 在地面设置分布 100 对通信终端。源终端和目的终端在地面的分布情况, 服从^[41]表 4-7。

表 4-7 地面终端分布情况 (%)

源终端	目的终端					
	北美	南美	欧洲	非洲	亚洲	大洋洲
北美	60	10	15	2	10	3
南美	35	40	12	2	8	3
欧洲	40	5	40	2	10	3
非洲	40	2	30	20	5	3
亚洲	30	2	10	2	50	6
大洋洲	40	2	10	2	12	34

然后, 对 LEO48 星座参数进行设定。如表 4-8 所示。

表 4-8 LEO48 星座仿真参数

核心参数	数值
高度 (km)	1450
轨道面数	6
单轨道面卫星数	8
最小仰角	10°
轨道倾角	86°
极区阈值	70°
ISL 队列类型	FIFO
ISL 队列长度 (Packets)	300
ISL 带宽 (Mb/s)	10
UDL 带宽 (Mb/s)	10

最后, 将 SLT 路由算法的基础路由模块周期性执行周期设定为 500ms, 动态信任评估处理模块的信任评估模型执行周期设定为 2s, 动态健康诊断处理模块的 Hello 数据包周期性发送间隔设定为 2s, Counter 值设定为 1。同时, 通过在协议源码中, 添加模拟恶意卫星行为的相关代码, 来得到恶意卫星节点。只有在 Otel 脚本中, 配置某些正常卫星为恶意卫星时, 模拟恶意卫星行为的代码才会运行。并

且把数据流周围大概率参与路由的关键卫星节点，设定为恶意卫星节点，可发动诸如黑洞、灰洞等攻击行为。最大恶意卫星节点数也限定为 10。

4.4.2 仿真结果分析

(1) 安全判定阈值 τ 的选定分析

判定某一卫星节点是否可信，需要选定一个合理的安全判定阈值 τ ，过大或过小都会影响 SLT 路由算法所带来的安全防护效益。因此，通过在 SLT 路由算法运行时设定不同阈值 τ ，用以测定 SLT 路由算法在运行时，具有最佳安全性能的最合理阈值 τ 的取值。此实验在 LEO48 星座网络中，共设有 5 颗恶意卫星节点。恶意卫星节点发生黑洞/灰洞攻击的概率为 0.65，发生修改攻击的概率为 0.35。同时，设定地面终端数据发送速率为 30packet/s，使得整个卫星网络处于轻负载运行。采用不同阈值 τ 进行测试，实验结果如图 4-15 所示。

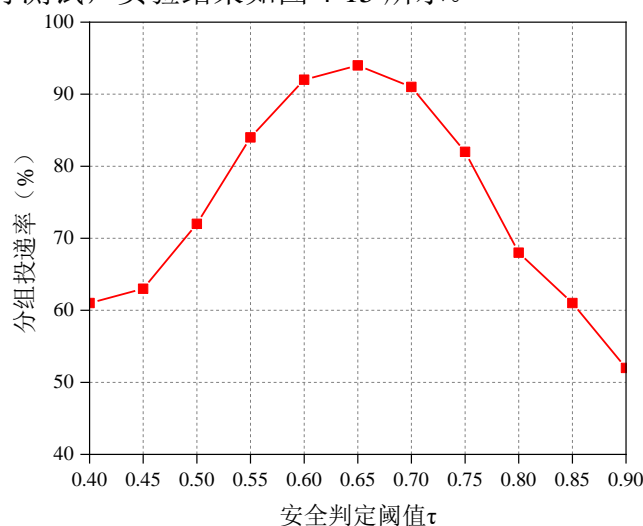


图 4-15 不同安全判定阈值 τ 下分组投递率变化图

分组投递率指的是，所有地面目的终端接收到的数据包个数与所有地面源终端发出的数据包总数比值。由图 4-15 可知。首先，当安全判定阈值 τ 取值较小时，分组投递率较低。此时，是因为阈值较低时，无法有效判定出恶意卫星节点，使得恶意卫星节点参与了正常的路由转发过程，造成了数据包的恶意丢失；然后，随着安全判阈值 τ 取值的不断增大，恶意卫星节点被有效地判定识别出来，并对其进行了及时隔离处置。因此，分组投递率得到了稳步增加，并在阈值 τ 取值为 0.65 时分组投递率均取得了最优值；但是，在阈值 τ 大于 0.65 后，分组投递率在逐步降低，并在阈值为 0.9 时，分组投递率达到了最低值，数据路由转发性能骤降。此时，是因为阈值 τ 设定地过高，正常的卫星节点也被误判为恶意的卫星节点。使得

能够参与到正常路由转发的卫星节点数骤降，流量都被过度地集中到少量的正常卫星上进行传输。卫星负载压力十分大，既而造成 ISL 发生拥塞，队列溢出大量数据包，造成了分组投递率的骤降。极大地影响了数据转发的性能。因此，最终选定最佳阈值 τ 为 0.65。

(2) 不同恶意卫星节点数下 SLT 路由算法安全性能分析

为了测试 SLT 路由算法的安全性能。此实验依旧设置地面终端数据发送速率为 30packet/s，使得整个卫星网络处于轻负载运行。同时，设定阈值 τ 为 0.65，恶意卫星节点发生黑洞/灰洞攻击的概率为 0.65，发生修改攻击的概率为 0.35。

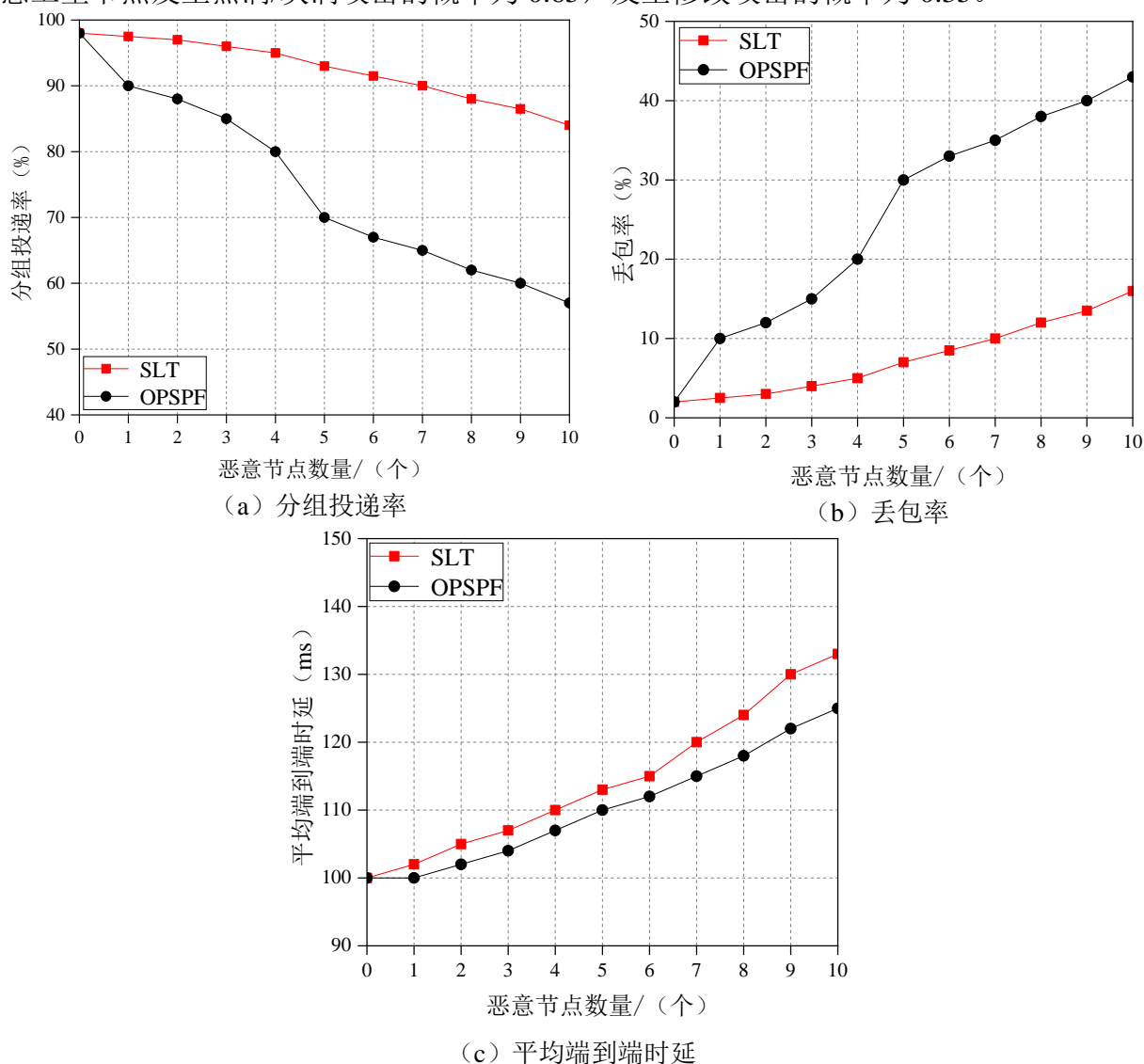


图 4-16 路由性能随恶意节点数量变化趋势图

通过设置不同的恶意卫星节点数，将本文提出的 SLT 安全路由算法与文献[44]所提出的基于轨道预测的 OPSPF 路由算法，在分组投递率、丢包率以及平均端到

端时延等方面,进行统计对比分析。测试验证 SLT 安全路由算法,在路由过程中所带来的安全效益。分组投递率的含义已在上述进行了解释。丢包率指的是未成功交付给地面目的终端的数据包个数与所有地面源终端发出的数据包总数比值。而平均端到端时延可由网络中所有的端到端通信时延,求平均得到。

由图 4-16 可知,加入基于 D-S 证据理论信任评估模型的 SLT 安全路由算法:在分组投递率方面,如图 4-16(a)所示。SLT 路由算法的分组投递率,整体都要比 OPSPF 路由算法高。且随着恶意卫星节点数的不断攀升,SLT 路由算法的分组投递率性能表现就越为出色;同时,两者在丢包率对比方面,如图 4-16(b)所示。SLT 路由算法的丢包率,也要明显小于 OPSPF 路由算法,这是由于 SLT 路由算法加入了动态信任评估模块,对卫星网络中的恶意卫星节点,进行了及时、有效地隔离与处置,避免了恶意节点所带来的持续恶意破坏影响。而 OPSPF 路由算法却认为,在整个卫星通信网络系统中,所有卫星节点都是完全可信的,无恶意卫星节点的存在。因此,会有恶意卫星节点加入正常的路由转发路径,发起诸如黑洞、灰洞等恶意攻击行为,造成数据包的恶意丢弃。因此,OPSPF 路由算法在分组投递率与丢包率方面的表现,均劣于本文所提出的 SLT 安全路由算法;但是,在传输时延对比方面,如图 4-16(c)所示。SLT 路由算法的表现却要差于 OPSPF 算法。这是由于 SLT 路由算法,为避开恶意卫星节点而选择了绕远,以牺牲传输跳数的代价,来换取数据包路由转发时的安全性能保证。因此,SLT 路由算法的平均端到端时延整体都要高于 OPSPF 算法。但是,时延性能还是在可接受的范围内。而且随着对恶意卫星节点的逐步有效隔离与处置,端到端时延会趋于平稳。

4.5 本章小结

为解决 LEO 卫星网络中潜在的内部路由攻击问题,通过考虑 LEO 卫星网络的内在运动特点以及在卫星网络中实现分布式动态信任评估的特殊性。本章从路由安全角度为切入点,提出设计了一种 SLT 安全路由算法。首先,提出设计了一种基于 D-S 证据理论的 LEO 卫星网络信任评估模型,此部分包括直接信任、间接信任以及聚合信任模型的设计;然后,采用此信任评估模型对一种低开销的基于轨道预测的 OPSPF 路由算法,进行信任安全加固改造。最终,得到本章所提出的 SLT 安全路由算法。SLT 算法具体可分为基础路由模块、动态信任评估处理模块以及动态健康诊断处理模块的设计;最后,采用 NS2 网络仿真软件,来完成 SLT 路由算法与 OPSPF 路由算法之间,在平均端到端时延、丢包率以及分组投递率等方面的安全性能对比分析。SLT 算法在丢包率以及分组投递率方面,均取得了不错的性能表现。但在平均端到端时延性能表现,略差于 OPSPF 算法。

第五章 全文总结与展望

5.1 全文总结

作为传统地面通信骨干网络的有力扩展与补充,卫星通信系统能够实现对偏远山区、沙漠、海洋等苛刻环境地区下无缝信号覆盖。其中,LEO 卫星通信网络系统更是凭借其低时延、研发与维护成本低、开发周期短等优势受到了各航天科技大国的重点关注与投入。但是,LEO 卫星网络所处的外太空环境较为恶劣与复杂。一方面面临高动态拓扑变化、全球流量分布不均衡、节点和链路易发生拥塞等问题的挑战;另一方面由于星间链路稳定性差,且因受自身开放性、暴露性等特点的影响,易遭受不法分子的恶意攻击。因此,如何实现数据在 LEO 卫星网络中的高效、可靠传输是本文重点关注的。针对以上两方面的问题,本文提出了各自的解决方案。

主要成果及结论总结如下:

(1)本文提出了一种基于 QoS 保障 LEO 卫星网路可靠性路由算法-RLQ 路由算法。从路径 QoS 保障以及全局流量均衡角度出发,较好地解决了卫星节点和链路拥塞问题。首先,GLSB 的更新建立由于采用了改进轨道发言人机制。因此,运行较为稳定且代价开销较小,优于基于全网洪泛方式的链路状态信息收集机制;然后,由于构建了一种多 QoS 约束且能够实现全球流量均匀分布的最优路由模型,能够在保证路径 QoS 前提下,从全局角度出发实现流量的均衡分布。提高非热点区域上空卫星使用率,轻量化热点区域上空卫星流量负载压力,减小拥塞发生概率,降低因拥塞导致队列溢出所产生的丢包,提高路由转发的可靠性。因此在平均端到端时延、丢包率、吞吐量以及流量均衡指数等方面,RLQ 算法均优于未考虑节点资源占用的 DT-DVTR 算法以及局部流量均衡的 ELB 算法;再然后,由于采用了拓扑剪枝预处理对多约束模型进行了求解降维。因此,通过一种基于代数迭代方式的拉格朗日松弛算法便可实现对此路由模型的快速求解;最后,通过路径信息压缩编码机制得到路径 ID 表,大大降低了路由表的存储与控制开销。

(2)本文提出了一种基于节点信任度的 LEO 卫星网路安全路由算法-SLT 路由算法。从路由安全角度出发,较好地解决了卫星网络中潜在的内部路由攻击问题。首先,基于 D-S 证据理论提出了一种 LEO 卫星网络的动态信任评估模型,此模型可不需要任何集中式或分布式可信基础措施,通过卫星节点的分布式协作便可实现节点信任度的更新;然后,同时考虑了 LEO 卫星网络的内在运动特点以及信任管理对于处理内部路由攻击的突出优势。因此,选定一种低开销的 OPSPF 算

法作为原料路由算法，采用本文提出的信任评估模型对其进行信任安全加固。最终，得到 SLT 算法。SLT 算法既继承了 OPSPF 算法中通过轨道预测方式，使之拥有处理规则拓扑变化时的低收敛开销优点，亦考虑了卫星网络中恶意卫星节点以及故障链路的存在。对发动如黑洞、灰洞等攻击的恶意节点进行及时隔离处置，以及对故障链路进行及时避让。因此，SLT 算法在分组投递率和丢包率方面，均优于 OPSPF 算法，降低了恶意节点恶意丢弃数据的影响，提高了路由转发的可靠性。但由于避让恶意卫星节点而选择了绕远。因此，SLT 算法在平均端到端时延性能表现，略差于 OPSPF 算法。

5.2 后续工作展望

本文分别从 QoS 保障角度以及路由安全角度出发，设计了两种不同的 LEO 卫星网络的可靠性路由算法。但是，对于本文所设计的两种可靠性星间路由算法，有待进一步研究，具体考虑如下：

（1）仿真实验有待加强和完善。针对 LEO 卫星网络中路由算法的性能验证，本文都是基于仿真软件及相关的仿真平台。而本文提出的两种可靠性路由算法运用在实际场景中，其真实效果有待进一步考究。因此，如何在真实的 LEO 卫星网络环境中，部署本文提出的可靠性路由算法，研发具有工程应用价值的可靠性星间路由算法，是亟待解决的问题。

（2）本文所提出的两种可靠性路由算法，都是采用单路径的方式完成数据的星间传输。但是，为了使星间路由具有更强的抗毁性以及动态适应性，后续研究可考虑设计为多路径传输的方式，更好地完成空间数据的可靠传输。

致 谢

行文至此，落笔为终。以昭求学之路漫漫，吾乃心系三年许，三千往事浮眼前。犹记得当年远从滨城，奔赴蓉城求学的欣喜，亦在三年间成长收获了许多。此刻，提笔致谢，心中不免有很多感慨与回味，沉甸而又厚重。

首先，感谢在三年读研期间，母校成电所给予的舒适生活环境、良好学习氛围。授课老师风趣幽默的讲解令我印象深刻，同学们认真学习的样子令我印象深刻。图书馆是我爱去的地方，在那里不仅能够找到科研相关的书籍资料，也能提供闲暇之余放松身心的名著小说。

十分感谢我的导师廖丹教授。在我成电三年的学习与生活中，各方面都给予了我最有力的帮助、理解与鼓励。在我学习、科研迷茫的时候，廖老师总会耐心、循循善诱地引导我思考，教会我分析、并逐步解开难题。也在廖老师身上学到了，严谨科研、敢于探索以及勤于思考的优秀品质，使我终生难忘、终生受益。

此外，特别感谢我的李慧师姐。在我科研无助的时候，总能给予我最细致、最有用的点拨与指导，使我信心倍增，能够继续开展后续研究。感谢新型网络小组中的每一员，韩钧师兄、高泽恺师兄、刘晓明师兄以及王文滔师弟，在每次例会时毫无保留的学术分享与建议。感谢我的好兄弟们，严鑫、贺元林和梁斯硕，是他们给予了我三年以来在成都的快乐与支持。也要感谢我的女朋友给予我那么多的欢声与笑语，使我每天开心快乐、幸福甜蜜。

最后，感谢我的爸妈，在我学习遇阻，找工作不顺的时候。爸妈总是能给予我最鼎力、最温暖的鼓励与支持。今后唯有努力工作，不断进步，不负大好青春韶华。

岁月悠悠，愿大家一切都好，一切顺利！

参考文献

- [1] D. Zhou, M. Sheng, K.-S. Lui, et al. Lifetime Maximization Routing with Guaranteed Congestion Level for Energy-Constrained LEO Satellite Networks[C]. 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, 2016, 1-5
- [2] M. Jiang, Y. Liu, W. Xu, et al. An Optimized Layered Routing Algorithm for GEO/LEO Hybrid Satellite Networks[C]. 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, 1153-1158
- [3] 纪明星. 天通一号卫星移动通信系统市场及应用分析[J]. 卫星与网络, 2018, 181(4): 42-43
- [4] R. J. Leopold. The Iridium Communications Systems[C]. [Proceedings] Singapore ICCS/ISITA92, Singapore, 1992, 451-455
- [5] R. A. Wiedeman, A. J. Viterbi. The Globalstar Mobile Satellite System for Worldwide Personal Communications[C]. Proc. of 3rd Int. Mobile Satellite Conference (IMSC'93), Washington, 1993, 285-290
- [6] D. P. Patterson. Teledesic: A Global Broadband Network[C]. 1998 IEEE Aerospace Conference Proceedings (Cat. No. 98TH8339), Snowmass, 1998, 547-552
- [7] 郭庆, 王振永, 顾学迈, 等. 卫星通信系统[M]. 北京: 电子工业出版社, 2010, 98-99
- [8] P. Sourisse. Skybridge: Global Multimedia Access[J]. Alcatel telecommunications review, 1999, 3: 228-237
- [9] V. L. Foreman, A. Siddiqi, O. De Weck. Large Satellite Constellation Orbital Debris Impacts: Case Studies of OneWeb and SpaceX Proposals[C]. AIAA SPACE and Astronautics Forum and Exposition, Orlando, 2017, 3086-3100
- [10] J. Foust. SpaceX's space-Internet woes: Despite technical glitches, the company plans to launch the first of nearly 12,000 satellites in 2019[J]. IEEE Spectrum, 2018, 56(1): 50-51
- [11] C. Sun, Y. Xiao, W. Zhao, et al. Development conception of space-ground integrated information network LEO mobile and broadband internet constellation[J]. Telecommunications science, 2017, 33(12): 43-52
- [12] 徐菁. “鸿雁”星座闪亮亮相移动通信或将全球无缝覆盖[J]. 中国航天, 2018, 487(11): 37-38
- [13] G. Katsoulis. Satellite telecommunications in the military: Advantages, Limitations and the Networking Challenge[M]. Berlin: Springer, 2014, 243-263
- [14] H. Yao, L. Shengnan, Y. Yan. Research on security transmission technologies for integrated satellite and terrestrial networks[C]. 2019 IEEE International Conference on Artificial

- Intelligence and Computer Applications (ICAICA), Dalian, 2019, 437-440
- [15] M. Werner. A dynamic routing concept for ATM-based satellite personal communication networks[J]. IEEE journal on selected areas in communications, 1997, 15(8): 1636-1648
- [16] E. Ekici, I. F. Akyildiz, M. D. Bender. A distributed routing algorithm for datagram traffic in LEO satellite networks[J]. IEEE/ACM Transactions on networking, 2001, 9(2): 137-147
- [17] H. Wang, Q. Zhang, X. Xin, et al. Cross-layer design and ant-colony optimization based routing algorithm for low earth orbit satellite networks[J]. China Communications, 2013, 10(10): 37-46
- [18] T. Taleb, D. Mashimo, A. Jamalipour, et al. Explicit Load Balancing Technique for N GEO Satellite IP Networks With On-Board Processing Capabilities[J]. IEEE/ACM transactions on Networking, 2008, 17(1): 281-293
- [19] G. Song, M. Chao, B. Yang, et al. Tlr: A Traffic-Light-Based Intelligent Routing Strategy for N GEO Satellite IP Networks[J]. IEEE Transactions on Wireless Communications, 2014, 13(6): 3380-3393
- [20] H. Wang, G. Wen, N. Liu, et al. A load balanced routing algorithm based on congestion for LEO satellite networks[J]. Cluster Computing, 2019, 22(4): 8025-8033
- [21] S. Karapantazis, E. Papapetrou, F.-N. Pavlidou. Multiservice on-demand routing in LEO satellite networks[J]. IEEE Transactions on wireless communications, 2009, 8(1): 107-112
- [22] Z. Jiang, C. Liu, S. He, et al. A QoS routing strategy using fuzzy logic for N GEO satellite IP networks[J]. Wireless Networks, 2018, 24(1): 295-307
- [23] X.W. Hao, J.F. Ma, F. Ren, et al. A kind of authentication routing protocol based on double satellite network in space information network[J]. Computer Science, 2011, 38(2): 79-81
- [24] J. Srinivas, S. Mukhopadhyay, D. Mishra. Secure and efficient user authentication scheme for multigateway wireless sensor networks[J]. Ad Hoc Networks, 2017, 54(1): 147-169
- [25] 彭长艳, 张权, 唐朝京. LEO 卫星网络中一种安全的按需路由协议[J]. 信号处理, 2010, 26(3): 337-346
- [26] C. Guo, J. Guo, C. Yu, et al. A Safe and Reliable Routing Mechanism of LEO Satellite Based on SDN[J]. CMC-COMPUTERS MATERIALS & CONTINUA, 2020, 64(1): 439-454
- [27] 李喆, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006, 27(8): 113-118
- [28] D. Yan, T. Tao, H. Xiongwen, et al. SRADR: Network Status and Reputation Adaptive QoS Dynamic Routing for Satellite Networks[C]. 2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, 2018, 1496-1500
- [29] Y.-H. Pan, T. Wang, Y. Wu, et al. Trust-based authentication routing protocol for satellite net-

- work[J]. Jisuanji Yingyong/ Journal of Computer Applications, 2011, 31(3): 781-783
- [30] 李广侠, 酆苏丹, 冯少栋. 切换保留信道与新呼叫排队相结合的 LEO 星座通信系统信道分配方案研究[J]. 通信学报, 2006, 27(9): 135-140
- [31] R. Radhakrishnan, W. W. Edmonson, F. Afghah, et al. Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view[J]. IEEE Communications Surveys & Tutorials, 2016, 18(4): 2442-2473
- [32] J. Bai, X. Lu, Z. Lu, et al. Compact explicit multi-path routing for LEO satellite networks[C]. 2005 Workshop on High Performance Switching and Routing, Hong Kong, 2005, 386-390
- [33] A. Svigelj, M. Mohorcic, G. Kandus, et al. Routing in ISL networks considering empirical IP traffic[J]. IEEE Journal on Selected areas in Communications, 2004, 22(2): 261-272
- [34] J. Bai, X. Lu, Z. Lu, et al. A distributed hierarchical routing protocol for non-GEO satellite networks[C]. Workshops on Mobile and Wireless Networking/High Performance Scientific, Engineering Computing/Network Design and Architecture/Optical Networks Control and Management/Ad Hoc and Sensor Networks/Compil, Montreal, 2004, 148-154
- [35] Z. Wang, J. Crowcroft. Quality-of-service routing for supporting multimedia applications[J]. IEEE Journal on selected areas in communications, 1996, 14(7): 1228-1234
- [36] A. Juttner, B. Szviatovski, I. Mécs, et al. Lagrange relaxation based method for the QoS routing problem[C]. Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213), Anchorage, 2001, 859-868
- [37] S. Kurkowski, T. Camp, N. Mushell, et al. A Visualization and Analysis Tool for NS_2 Wireless Simulations: inspect[C]. 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, Atlanta, 2005, 503-506
- [38] A. M. AbuMahfouz, G. P. Hancke. NS_2 extension to simulate localization system in wireless sensor networks[C]. IEEE Africon'11, Victoria Falls, 2011, 1-7
- [39] 杨颖, 王琦. STK 在计算机仿真中的应用[M]. 北京: 国防工业出版社, 2005, 15-35
- [40] 陈敏. OPNET 网络仿真[M]. 北京: 清华大学出版社, 2004, 10-36
- [41] M. Mohorcic, M. Werner, A. Svigelj, et al. Adaptive routing for packet-oriented intersatellite link networks: performance in various traffic scenarios[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 808-818
- [42] Y. Rao, R.c. Wang. Agent-based load balancing routing for LEO satellite networks[J]. Computer networks, 2010, 54(17): 3187-3195

- [43] 关汉男. 基于 LEO 的空间网络安全体系及关键技术研究[D]. 上海: 上海交通大学, 2014, 14-16
- [44] T. Pan, T. Huang, X. Li, et al. OPSPF: Orbit Prediction Shortest Path First Routing for Resilient LEO Satellite Networks[C]. ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, 2019, 1-6
- [45] A. P. Dempster. Upper and Lower Probabilities Induced by a Multivalued Mapping[J]. Annals of Mathematical Statistic, 1967, 38(2): 325-339
- [46] G. Shafer. A mathematical theory of evidence[M]. New York: Princeton University Press, 1976, 178-183
- [47] A.-L. Jousselme, D. Grenier, É. Bossé. A new distance between two bodies of evidence[J]. Information fusion, 2001, 2(2): 91-101
- [48] T. Han, S. Luo, H. Zhu, et al. Trust routing algorithm based on multiple decision factor theory in OSPF protocol[J]. The Journal of China Universities of Posts and Telecommunications, 2013, 20(5): 104-109
- [49] 叶阿勇, 马建峰. 一种移动自组网中信任评估模型的设计[J]. 计算机研究与发展, 2008, 45(5): 765-771
- [50] S. R. Zakhary, M. Radenkovic. Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments[C]. 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS), Kranjska Gora, 2010, 161-167
- [51] Q. Jing, L. Tang, Z. Chen. Trust Management in Wireless Sensor Networks[J]. Journal of Software, 2008, 19(7): 1716-173
- [52] C. K. Murphy. Combining belief functions when evidence conflicts[J]. Decision support systems, 2000, 29(1): 1-9
- [53] 陈一雷, 王俊杰. 一种 D-S 证据推理的改进方法[J]. 系统仿真学报, 2004, 16(1): 28-30
- [54] 毕梦格, 巨玉, 侯蓉晖. 一种环境自适应的卫星网络安全路由协议[J]. 西安电子科技大学学报, 2020, 47(1): 66-72
- [55] 郑静. 空间网络安全路由的设计与仿真实现[D]. 西安: 西安电子科技大学, 2017, 23-27
- [56] Z. Yu, H. Zhou, Z. Wu. A trust-based secure routing protocol for multi-layered satellite networks[C]. 2012 IEEE International Conference on Information Science and Technology, Wuhan, 2012, 313-317

攻读硕士学位期间取得的成果

授权和申请专利：

- [1] 廖丹, **李航**, 李慧, 张明, 李玉娟。基于改进蚁群的 SDN 卫星网络多 QoS 约束路由方法, ZL201911003387.5, 授权日: 2020.7.17
- [2] 廖丹, **李航**, 王文滔, 李慧, 陈雪, 张明。基于 QoS 保障的 LEO 卫星网络可靠性路由方法, CN202010907402.5, 申请日: 2020.9.2
- [3] **李航**, 杨凡德, 廖丹, 简平, 王文滔, 李慧。一种基于节点信任度的 LEO 卫星网络安全路由方法, CN202110323785.6, 申请日: 2021.3.26

参与项目：

- [1] 中央高校基本科研业务费项目“基于软件定义的卫星网络研究”，项目编号：ZYGX2019J125, 2019.1-2020.12
- [2] 电子信息装备体系研究国防科技重点实验室基础研究项目“面向战场态势感知的卫星物联网研究”，项目编号：DXZT-JC-ZZ-2017-012, 2020.8-2021.7
- [3] 四川省科技厅项目“5G 卫星物联网的路由及资源优化研究”，项目编号：2021YFG0150, 2021.1-2022.12

学业奖励：

- [1] 2018 年获研究生二等奖学金
- [2] 2019 年获研究生三等奖学金
- [3] 2020 年获研究生二等奖学金