基于跨域网联态势的多星座信任管理研究

宋宇杰[1]，曹越[1]，高骏峤[1]，赵亮[2]，李立[3]，孙智立[4]
（1. 武汉大学国家网络安全学院，湖北 武汉 430070；2. 沈阳航空航天大学计算机学院，辽宁 沈阳 110136；
3. 西北工业大学电子信息学院，陕西 西安 710129；4. 萨里大学通信系统研究所，吉尔福德 英国 GU2 7XH）

摘 要：随着卫星互联网在通信与组网方面的快速发展，跨域异构卫星相互建立链路并提供多样化数据服务，给卫星互联网安全带来了信任评估不准与卫星跨域不互信的挑战，因此，构建信任体系对卫星进行信任评估显得尤为重要。针对如何基于跨域网联态势与多维度信任观点动态评估卫星可信度，提出了一项基于跨域网联态势的多星座信任管理方案。该方案针对多星座场景，考虑多维度信任观点，设计分位图信任过滤机制，利用权重和方法聚合信任观点与信任阈值，最终判别卫星的可信度。实验结果表明，该方案的准确率、精确率、召回率与 F 值均优于其他基准算法。

关键词：卫星互联网；卫星星座；信任管理
中图分类号：TN915.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00477

Research on cross-domain network situation-based trust management in multiple constellations

SONG Yujie[1], CAO Yue[1], GAO Junqiao[1], ZHAO Liang[2], LI Li[3], SUN Zhili[4]
1. School of Cyber Science and Engineering, Wuhan University, Wuhan 430070, China
2. School of Computer Science, Shenyang Aerospace University, Shenyang 110136, China
3. School of Electronics and Information, Northwestern Polytechnical University, Xi’an 710129, China
4. Institute of Communication Systems, University of Surrey, Guildford GU2 7XH, U.K.

Abstract: With the rapid development of communication and networking technologies in satellite networks, cross-domain heterogenous satellites establish connectivity with each other and provide various data services, which bring serious challenges to satellite networks, such as inaccurate trust evaluation and cross-domain mistrust of satellites. Therefore, it is particularly important to build a trust system to evaluate trust of satellites. To evaluate the trustworthiness of satellites based on cross-domain network situation and multi-dimensional trust opinions, a cross-domain network situation-based trust management in multiple constellations was proposed. The multi-dimensional trust opinions in multiple constellations was considered, and quantile-quantile plot trust filtering mechanism was designed. Then, trust opinions and trust thresholds were weighted to identify the trustworthiness of satellites. Experiment results show that the proposed method outperforms baselines in terms of accuracy, precision, recall, and F-value.

Key words: satellite Internet, satellite constellation, trust management

收稿日期：2024−12−29；**修回日期：**2025−02−19
通信作者：曹越，yue.cao@whu.edu.cn
基金项目：国家重点研发计划（No.2022YFE0139300）；广东省基础与应用基础研究基金资助项目（No.2022B1515120067）
Foundation Items: The National Key Research and Development Program of China (No. 2022YFE0139300), Guangdong Basic and Applied Basic Research Foundation (No. 2022B1515120067)

0 引言

随着通信技术与空天技术的迅速发展，多样化场景创新的应用需求增加，使得卫星互联网受到广泛关注[1-2]。卫星互联网由于具有空间优势与多场景适配能力，成为发展未来网络、赋能全球通信的关键技术途径，为实现全域覆盖（如地域、网域）、全方位、立体数据服务提供了高效的解决方案[3-5]。卫星互联网由众多卫星星座组成，通过共同协作的方式完成特定任务，如跨域通信、实时导航、高精度定位等[6-7]。卫星星座由多颗卫星组成，在空间上以特定的构型分布，如北斗星座、千帆星座、伽利略卫星星座、星链等。

全域覆盖通信服务、星载数据处理、高精度地图服务等应用需求随卫星互联网的发展应运而生[8-9]，上述新型数字服务依赖于星间负载均衡、动态链路管理、服务能力量化、信任评估等技术[10-13]。尽管现有卫星互联网在组网与通信方面的研究趋于成熟，但其研究重点仅局限于单层卫星互联网或单一星座场景，无法适配复杂网联态势的多星座场景，难以满足服务区分的高效数据服务需求。其次，现有卫星互联网安全的研究注重通信链路安全风险，聚焦处理外部安全风险，缺乏从网络层面量化评估内部网络实体（卫星）的可靠性[14-15]。由于卫星的高速移动性，卫星互联网拓扑频变、海量数据互传，基于链路的通信安全检测策略难以满足可信度评估的高实时性需求。因此，如何利用卫星互联网网联态势实现卫星可信度评估，已成为攻克上述问题的重要挑战。

当前，现有卫星互联网中与信任安全相关的研究聚焦安全路由与信任管理，以提升数据传输可靠性与网络安全性[16]。其中，安全路由相关研究通过评估网络链路可信度与负载，以提升网络数据传输的可靠性[17]。与信任管理相关研究考虑直接信任（评估卫星对被评估卫星的信任）与间接信任（评估卫星的邻居卫星对被评估卫星的信任），通过权重和方法聚合信任，构建信任模型，以识别网络实体的可信度[18]。然而，上述研究受限于网络拓扑、链路状态、数据交互等信息，且未有效动态调整信任阈值，导致信任评估不准确。因此，如何基于跨域网联态势与多维度信任观点动态评估卫星可信度，识别恶意网络实体（卫星），实现多星座信任管理，是卫星互联网安全研究领域亟待解决的关键问题。

基于此，针对如何保证卫星互联网可信数据传输服务问题，本文提出基于跨域网联态势的多星座信任管理方案（CDNS-TM, cross-domain network situation-based trust management in multiple constellations），以实现准确的卫星可信度评估，提高识别准确率、精确率、召回率与F值。本文主要贡献如下：

1)针对多星座卫星互联网场景，考虑动态构建信任场与权重场，建立分位图信任过滤机制，优化多维度信任观点有效性，以准确评估卫星可信度；

2)设计了动态拓扑适配的信任阈值聚合与信任相似度评估方法，解决传统信任管理采用固定信任阈值所造成的评估不准确问题，并从自证角度拓展信任评估方法的新途径，以提升信任评估的可靠性；

3)与基准算法相比，验证了CDNS-TM在准确率、精确率、召回率与F值方面的有效性。上述指标均值分别达到了99.52%、98.48%、99.99%与0.992 2。

1 相关工作

1.1 卫星互联网信任管理

现有卫星互联网安全中的与信任管理相关研究聚焦安全路由、可信链路构建与信任建模等应用[19-28]。其本质是通过数据交互建立信任关系，利用信任聚合手段实现信任评估，支撑可信组网、可靠链路建立及数据有效传输等应用，满足用户对可信环境的需求。

为支撑卫星互联网数据有效传输，现有相关研究开展了适配卫星互联网的安全路由协议、链路切换等研究。文献[19]提出了一项基于节点信任的低轨（LEO, low earth orbit）卫星网络安全路由算法，通过分布式信任评估模型和证据理论（DS, dempster-shafer）计算节点间信任值，并结合安全包转发路由协议，有效提升了网络的生存能力和数据传输的可靠性。文献[20]提出了一项可信自组织按需距离向量的安全路由协议，通过融合信任评估和负载均衡，增强卫星网络的路由安全性，有效抵御恶意节点攻击。文献[21]提出了一项基于信任的多层卫星网络安全路由协议，通过融合认证与信任机制，提

高路由安全性，同时考虑基于身份的签名算法，降低网络计算开销。文献[22]提出了一项针对超密集低轨道卫星网络的用户中心切换方案，该方案通过在多颗卫星中缓冲用户的下行数据，以支撑无缝切换。文献[23]提出了一项基于信道建模的多层星地融合数据分配策略，依托信誉框架，通过构建星载数据分配策略确认机制，提升数据分配策略的有效性，避免数据传输中断。文献[24]针对空天地一体化数据传输高时延问题，提出了一项在资源受限条件下的缓存优化与用户选择算法，旨在最大化剩余能源，同时设计了一种动态缓存适配的用户选择算法以优化数据传输。为解决拓扑频变、能源受限条件下海量空间数据卸载问题，文献[25]提出了一项在线数据卸载与功耗联合优化算法，利用双时间尺度时间扩展图抽取网络拓扑，并构建随机优化问题获得最优解。文献[26]提出了一项基于网络功能虚拟化的服务恢复模型，将任务管理问题转化为服务功能链部署问题，通过快速选择备用资源以完成部署，再将服务恢复问题构建为最小化时延开销问题，设计基于匹配博弈的求解算法，实现空天地一体化网络服务恢复。

在卫星网络数据传输的基础上，与信任管理相关研究基于贝叶斯理论构建信任模型，通过考虑多维度信任衡量观点，聚合信任观点，实现信任评估与管理。文献[27]提出了一项基于认证与资源切片访问的信任管理方案，考虑多维度直接信任与推荐信任，利用多重权重和方法聚合直接信任与间接信任，评估卫星综合信任值。文献[28]提出了一项基于信道感知的星地融合切换管理方案，通过构建星地信誉架构，考虑通信质量与卫星剩余服务时间，量化卫星服务能力，动态编排数据分配策略，实现星地数据可信传输。文献[29]提出了一项基于转发证据的去中心化信任管理方案，考虑转发证据与节点能耗，构建信任评估体系，过滤卫星网络中的恶意节点。文献[30]提出了一项LEO卫星互联网分布式信任管理机制，考虑直接信任与推荐信任，基于证据理论计算卫星的可信度，并根据信任值判断卫星的可信度。文献[31]提出了一项空天地一体化场景下的信任评估方案，基于贝叶斯理论，考虑了自信度（卫星对自身信任观点的准确度的认知）、信任向量与授权传播，并采用权重和方法计算信任值。文献[32]提出了一项基于直接非循环图的区块链辅助信任架构，该架构考虑网络实体计算能力与数据传输结果评估网络实体的信任值，同时利用区块链确保了信任值在跨域范围内的可验证性。为了解决多种恶意行为造成的信任危机，文献[33]提出了一项基于机器学习与数据融合的信任管理方法，考虑时空逻辑特征、行为特征与交通流特征，构建信任映射，以预测网络实体的信任度。文献[34]提出了一项基于模糊逻辑的动态信任管理方案，利用第2类型模糊逻辑方法融合多维度信任证据，以准确识别网络实体是否可信。

尽管上述研究针对如何准确评估网络实体的可信度问题进行了大量的探索，但仍面临网络拓扑频变、跨域实体不互信、信任评估不准确等问题。其次，由于信任维度不足、信任阈值固化，传统信任管理方案难以适配新型网络架构（卫星互联网）。因此，如何在卫星互联网场景下构建动态适配的可靠信任模型以支撑卫星互联网可信数据传输成为重要挑战。

1.2　安全威胁模型

在卫星互联网中，恶意卫星执行消息篡改攻击、坏嘴攻击与共谋攻击[35]，即恶意卫星将篡改接收的消息，并为其他卫星提供虚假信任观点。其中，当被评估卫星为正常卫星（良性卫星）时，恶意卫星为其提供较低的信任观点；当被评估卫星为恶意卫星时，恶意卫星为其提供较高的信任观点，以干扰正常卫星对其他卫星的信任评估准确性。

2　系统模型

2.1　系统架构

本文针对由不同高程的卫星组成的多星座卫星互联网，构建基于跨域网联态势的多星座信任管理的场景架构。多星座卫星互联网的系统架构如图1所示，其由多个卫星星座组成，每个星座有多颗卫星。卫星可划分为良性卫星与恶意卫星，恶意卫星会执行恶意行为，影响数据传输。卫星通过通信链路建立连接，包括星座内（域内）通信链路与星座间（域间）通信链路。其中，星座内通信链路为星座内卫星的数据服务提供传输途径；星座间卫星的数据服务通过域间通信链路实现。其次，各星座卫星随机生成海量数据，基于历史交互记录，计算卫星的多维度信任值，评估卫星及星座可信度，通过星座内/间通信链路将数据传输至目的卫星。

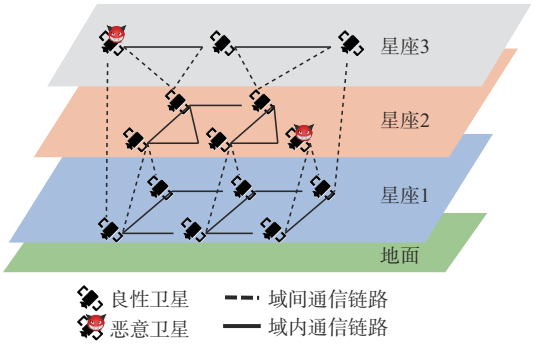


图1　多星座卫星互联网的系统架构

假设n个星座具备不同拓扑结构，表示为$G=\{C_1, C_2, \cdots, C_n\}$。由于每个星座的拓扑结构不同，星座中卫星的数量不一致，假设星座中卫星数量为m，其范式表示为$C_i=\{s_1, s_2, \cdots, s_m\}$，其中$s_m$表示第$m$颗卫星。其次，不同星座中卫星运行在不同高程的轨道上，如LEO星座中LEO卫星组成运行于500～2 000 km的轨道中，中轨（MEO, medium earth orbit）星座中MEO卫星运行于10 355 km的轨道中。此外，卫星基于自由空间光通信与其他卫星建立连接，并采用密集波分复用技术[36]聚合吞吐量，以满足高效数据传输需求。

2.2　信任模型

为保障跨域星座数据服务的可靠性，本文通过构建适配多星座场景的信任模型，考虑多维度信任观点，如直接信任、间接信任、星座信任等。卫星s_i的信任观点集合可构建信任场，计算式为

$$\boldsymbol{T}_i=\begin{bmatrix} T_{i,1}^1 & T_{i,1}^2 & \cdots & T_{i,1}^l \\ T_{i,2}^1 & T_{i,2}^2 & \cdots & T_{i,2}^l \\ \vdots & \vdots & \ddots & \vdots \\ T_{i,u}^1 & T_{i,u}^2 & \cdots & T_{i,u}^l \end{bmatrix} \tag{1}$$

其中，l表示信任维度，$T_{i,j}^l$表示s_i对卫星s_j在第l维度的信任值，u表示卫星总数量。为量化各维度信任的影响力，采用与信任场相同维度的权重场，卫星s_i的各维度信任权重的计算式为

$$\boldsymbol{W}_i=\begin{bmatrix} w_{i,1}^1 & w_{i,1}^2 & \cdots & w_{i,1}^l \\ w_{i,2}^1 & w_{i,2}^2 & \cdots & w_{i,2}^l \\ \vdots & \vdots & \ddots & \vdots \\ w_{i,u}^1 & w_{i,u}^2 & \cdots & w_{i,u}^l \end{bmatrix} \tag{2}$$

其中，$w_{i,j}^l$表示卫星s_i对卫星s_j在第l维度的信任权重，计算式为

$$w_{i,j}^l=\frac{T_{i,j}^l}{\sum_k^O T_{i,k}^l} \tag{3}$$

其中，O表示卫星s_i的邻居卫星集合，权重随着卫星链路变化（建立/断开链接）而变化，$T_{i,j}^l$表示卫星s_i对卫星s_j在第l维度的信任值。

从多维度评估卫星及星座的可信度，包括直接信任、间接信任、星座信任、综合信任、自证信任等。上述信任类型及关系如图2所示。$T_{i,j}$表示卫星s_i对卫星s_j的直接信任观点，计算式为

$$T_{i,j}=\frac{\alpha+1}{\alpha+\beta+2} \tag{4}$$

其中，α表示成功交互计数，β表示失败交互计数。

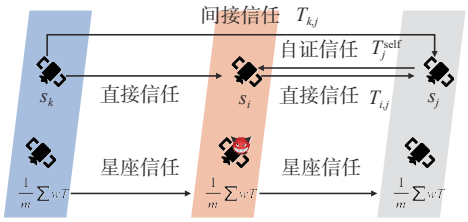


图2　信任类型及关系

若卫星s_k与卫星s_i存在通信链路（即邻居关系），s_k为s_i提供其对s_j的直接信任观点，该观点是间接信任（$T_{k,j}$）。其次，星座信任从宏观角度体现了域的可信度，依赖于星座中参与过数据服务的卫星的数据交互总量及其交互结果，计算式为

$$T^{C_k}=\frac{1}{m}\sum_i^{|C_k|} w_i T_i \tag{5}$$

其中，C_k表示第k个星座，T_i表示卫星s_i的信任值，w_i表示s_i的权重，$w_i=\dfrac{T_i}{\sum T_i}$。

根据直接信任、间接信任与星座信任的信任值，通过权重和方式聚合信任，即综合信任，计算式为

$$\boldsymbol{T}_i^{\mathrm{A}}=\boldsymbol{W}_i^{\mathrm{T}}\boldsymbol{T}_i \tag{6}$$

其中，$\boldsymbol{W}_i^{\mathrm{T}}$表示权重场$\boldsymbol{W}_i$的转置。基于此，评估卫星$s_i$对被评估卫星$s_j$的综合信任表示为$T_{i,j}^{\mathrm{A}}$。

由于卫星互联网中存在恶意卫星（被入侵的卫星），恶意卫星会提供虚假间接信任，即为恶意卫星提供较高的信任值（共谋攻击），为良性卫星提供较低的信任值（坏嘴攻击）。为减缓共谋攻击与坏嘴攻击的影响，基于跨域网联态势与历史交互信息，评估卫星s_i利用分位图过滤邻居卫星s_k提供的信任值。首先，假设邻居卫星集合为O，根据邻居卫星提供信任值及其可信度，计算权重化信任值$T'_{k,j}$，计算式为

$$T'_{k,j}=w'_{i,k}T_{k,j} \tag{7}$$

其中，$w'_{i,k}=w_{i,k}/\sum_h^O w_{i,h}$表示邻居卫星$s_k$的提供观

点对评估卫星s_i的重要程度，$w_{i,k}$表示s_i对s_k的信任权重，$w_{i,h}$表示s_i对s_h的信任权重。基于此，邻居卫星集合的信任序列可以表示为$\boldsymbol{T}_j^O=\left[T'_{1,j},T'_{2,j},\cdots,T'_{|O|,j}\right]$，并按升序排列，再分别统计下四分位数$Q_1$、中位数$Q_2$、上四分位数$Q_3$。随后，根据$Q_1$与$Q_3$计算四分位距（IQR），计算式为

$$\mathrm{IQR}=Q_3-Q_1 \tag{8}$$

评估卫星s_i可判断邻居卫星s_k提供的间接信任是否为异常值，判断式为

$$T'_{k,j}\in\left[Q_1-1.5\mathrm{IQR},Q_3+1.5\mathrm{IQR}\right] \tag{9}$$

若间接信任介于式(9)范围内，则表示间接信任正常；反之，间接信任存在异常，s_i并不考虑该信任值。若信任观点数量不超过3个，则考虑所有信任观点，以综合评估信任值。

此外，为增强信任评估的可靠性，本文利用卫星互联网场景中拓扑频变特征，提出了自证信任。由于卫星具有高速移动性，被评估的卫星s_j难以估计哪些卫星将为评估卫星s_i提供间接信任，进而无法准确计算出s_i对s_j的评估结果与自证信任之间的差值。因此，自证信任能够增强信任评估的可靠性，判断卫星是否提供虚假信任值。基于此，自证信任T_j^{self}表示卫星s_j对其自身的信任评估，考虑交互成功率与推荐有效性。其中，交互成功率表示卫星s_j与其他卫星成功交互的占比，推荐有效性表示该卫星为其他卫星提供了正确信任观点的占比。自证信任计算式为

$$T_j^{\mathrm{self}}=\left[w_1,w_2\right]\begin{bmatrix}T_j^{\mathrm{com}}\\T_j^{\mathrm{re}}\end{bmatrix} \tag{10}$$

其中，$T_j^{\mathrm{com}}=\dfrac{\alpha_j+1}{\alpha_j+\beta_j+2}$表示交互成功率的信任值，$\alpha_j$表示$s_j$的成功交互计数，$\beta_j$表示$s_j$的失败交互计数。$T_j^{\mathrm{re}}=\dfrac{\mathrm{rs}_j+1}{\mathrm{rs}_j+\mathrm{rf}_j+2}$表示推荐有效性的信任值，$\mathrm{rs}_j$与$\mathrm{rf}_j$表示$s_j$的真实推荐计数与虚假推荐计数。权重$w_1$与$w_2$采用熵权法计算，首先计算信息熵为

$$E_i=-\frac{1}{\ln m}p_i\ln p_i \tag{11}$$

其中，m表示自证信任的考虑因素维度，p_i表示T_j^{com}或T_j^{re}。其次，基于各个维度信任评估的信息熵，计算自证信任权重值，其计算式为

$$w_i=\frac{1-E_i}{\sum_k^m(1-E_k)} \tag{12}$$

其中，E_i、E_k分别表示第i个信息熵与第k个信息熵。

为判断被评估卫星提供的自证信任的接受程度，自证信任与综合信任的相似度计算式为

$$TS_{i,j}=1-\left|T_j^{\mathrm{self}}-T_{i,j}^{\mathrm{A}}\right|\geqslant\mu \tag{13}$$

其中，$T_{i,j}^{\mathrm{A}}$表示评估卫星s_i对被评估卫星s_j的综合信任，μ表示s_i对信任偏差的可接受阈值，即聚合信任阈值。若信任相似度大于或等于阈值μ，则表示s_j所提供的自证信任可被s_i接受；反之，则说明s_j提供了虚假自证信息。

基于卫星互联网的拓扑频变特征，为确保式(13)的有效性，阈值μ随着拓扑结构的变化而变化，且受到卫星自信度的影响，计算式为

$$\mu=\gamma\mu_{i,j}+\left(1-\gamma\right)\sum_k^{O'}w'_{i,k}\mu_{k,j} \tag{14}$$

其中，γ表示卫星s_i的自信度，O'表示经过式(9)过滤之后的有效邻居卫星集合，$w'_{i,k}$表示O'中计算的权重，$\mu_{k,j}$表示邻居卫星s_k对被评估卫星s_j的信任阈值。

同时，卫星的自信度受到其判断结果的影响，根据该结果动态调整自信度，以更加准确地判断自身观点与来自其他卫星观点的重要性，计算式为

$$\gamma=\gamma^0+\frac{\alpha-\beta}{\alpha+\beta+2} \tag{15}$$

其中，γ^0表示初始化自信度值，其取值范围为[0.5, 0.55]。α表示该卫星的成功交互计数，β表示该卫星的失败交互计数。

此外，为提升信任评估的准确性，卫星根据邻居卫星、星座信任及数据传输结果动态调整其信任观点，计算式为

$$T_{i,j}^{l*}=\gamma T_{i,j}^{l}+\left(1-\gamma\right)\frac{\left|\sum_k^{O'}w_{i,k}T_{k,j}^{l}-T_{i,k}^{l}\right|}{\max\left\{\sum_k^{O'}w_{i,k}T_{k,j}^{l},T_{i,j}^{l}\right\}} \tag{16}$$

3　算法设计

图3展示了CDNS-TM的算法技术路线。首先，各星座中卫星动态感知网联态势，构建信任场及其权重场（算法1）；其次，根据网络拓扑与间接信任观点，构建分位图信任过滤机制（算法2）；再次，基于过滤后的信任场与权重场，计算卫星的综合信任值；随后，根据综合信任、自证信任与信任阈值，判断卫星是否可信（算法3）；最后，实时维护卫星的信任观点（算法4）。其中，算法1与算法2

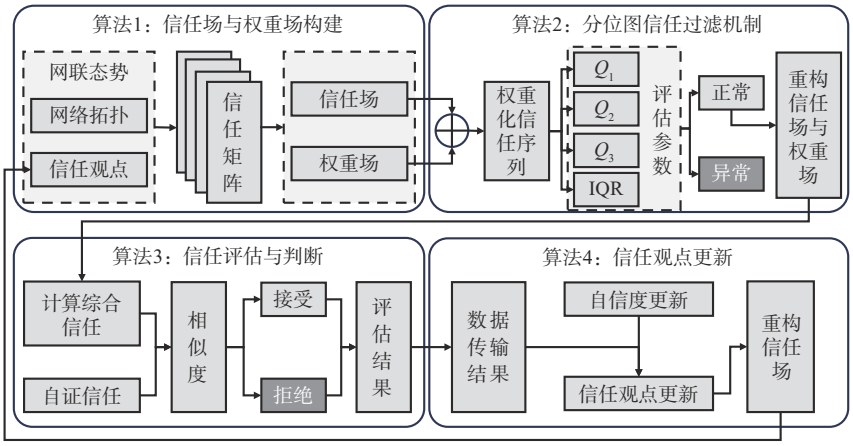


图3　CDNS-TM的算法技术路线

为算法3提供可靠信任观点，算法4动态更新信任观点，为后续信任评估提供了更加准确的观点，确保信任评估的可靠性。

3.1　信任场与权重场构建

由于卫星具有高速移动性，卫星互联网的网联态势频变，卫星需通过链路管理动态感知网络拓扑，为信任评估提供物理与信息域的数据支持。算法1描述了基于网联态势的信任场与权重场构建过程：首先，卫星基于网络拓扑与链路信息，根据式(4)计算与之建立连接的卫星的信任观点，构建与网络拓扑适配的多维异构信任矩阵；其次，根据网络拓扑与信任矩阵，根据式(3)计算信任观点的权重值，完成信任场与权重场构建。

算法1　信任场与权重场构建

输出：信任场、权重场

卫星与视野范围内的其他卫星建立连接，并动态构建网络拓扑；

基于历史交互记录，卫星根据式(4)计算对其他卫星的信任值；

根据式(1)，构建多维异构信任矩阵，形成信任场；

基于网络拓扑与信任矩阵，根据式(3)计算信任观点的权重值；

根据式(2)完成权重场构建；

输出信任场与权重场。

3.2　分位图信任过滤机制

由于被入侵的卫星会提供虚假的信任观点，卫星需要过滤掉此类异常数据，以提升信任评估的可靠性。算法2描述了利用分位图过滤信任观点的过程。首先，卫星根据信任场与权重场信息，计算权重化信任值，并按升序排列。其次，分别计算Q_1、Q_2、Q_3与四分位距IQR。再次，若权重化信任值满足式(9)要求，则该信任观点为正常，得以保留；反之，则该信任为异常，将其过滤。最后，根据算法1重新构建信任场与权重场。

算法2　分位图信任过滤机制

输入：信任场、权重场

输出：过滤后的信任场、权重场

根据式(7)，计算权重化信任值，并按照升序排列；

分别计算Q_1、Q_2、Q_3，并根据式(8)，计算IQR；

根据式(9)，过滤不满足要求的信任观点；

根据式(1)与式(2)重构信任场与权重场；

输出过滤后的信任场与权重场。

3.3　信任评估与判断

为避免恶意卫星篡改、丢弃数据，根据信任场、权重场、自证信任与信任阈值，卫星评估邻居卫星的信任度，以判断邻居卫星的可靠性。算法3描述了信任评估与判断的详细过程：首先，根据算法2输出的信任场与权重场，卫星计算被评估卫星的综合信任；其次，根据被评估卫星的自证信任，卫星评估综合信任与自证信任之间的相似度；最后，卫星计算聚合信任阈值，以判断相似度是否可被接受，即相似度大于或等于信任阈值，表示被评估卫星可信，反之，则表示被评估卫星不可信。

算法3　信任评估与判断

输入：过滤后的信任场、权重场

输出：信任评估结果

根据式(6)，计算被评估卫星的综合信任；

根据式(10)，计算被评估卫星的自证信任；

根据式(13)，计算被评估卫星的自证信任与其综合信任的相似度；

根据式(14)，计算聚合信任阈值，并判断相似度是否可被接受。

输出信任评估结果。

3.4　信任观点更新

为确保信任评估与判断的准确性，卫星动态更新其信任观点，以支撑卫星互联网安全运维。算法4描述了卫星的信任观点更新过程：首先，根据数据传输结果，卫星动态更新其自信度，以更准确地聚合信任观点；其次，卫星根据信任场与数据传输结果，计算信任观点。

算法4　信任观点更新

输入：信任场、数据传输结果

输出：更新后的信任观点

根据数据传输结果与式(15)，计算卫星的自信度；

根据式(16)，计算卫星对其邻居卫星的信任观点；

按照算法1重构信任场；

输出更新后的信任观点。

4　性能评估

4.1　仿真设置

仿真实验在机会网络环境仿真器[37]中实现，根据文献[23,27-28,30]参数配置，仿真详细参数设置见表1。

表1　　仿真详细参数设置

参数	参数设置
仿真场景/m×m	40 074 156×20 037 078
仿真时长/s	18 000
卫星数量/个	170
星座数量/个	4
卫星高程/km	500～10 355
初始化信任值	0.5
初始化自信度	0.5
信任阈值	[0.45, 0.55]
数据量/个	[3 600~18 000]
数据大小/MB	100

其中，仿真场景按墨卡托投影配置等比例地球模型，仿真时间为18 000 s。卫星根据其不同星座归属性，分布于不同高程（500～2 000 km、10 355 km），其运行速度由万有引力公式得出，即 $F=\frac{GM_{\mathrm{e}}m_{\mathrm{s}}}{R+H}=\frac{m_{\mathrm{s}}v^2}{R+H}$，其中 G、M_{e} 与 m_{s} 分别代表万有引力常量、地球质量与卫星质量，R 为地球半径，H 为卫星高程。初始化信任值设为0.5，初始信任阈值从[0.4, 0.5]中选取，初始自信度为0.5。此外，卫星基于自由空间光通信技术[38]实现卫星/星座间通信，并以此组建卫星互联网。

4.2　性能指标

准确率表示正确识别次数与总识别次数的比值，计算如下

$$\mathrm{Accuracy}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{17}$$

其中，TP表示正确识别正样本（良性卫星）的数量，TN表示正确识别负样本（恶意卫星）的数量，FP表示错误识别为正样本的数量，FN表示错误识别为负样本的数量。

精确率表示识别结果中真实为正样本计数与识别为正样本计数的比值，计算如下

$$\mathrm{Precision}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \tag{18}$$

召回率表示识别结果中真实为正样本计数与总正样本计数的比值，计算如下

$$\mathrm{Recall}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{19}$$

F值表示根据精确率与召回率综合衡量识别的性能，计算如下

$$F_{\sigma}=\left(1+\sigma^2\right)\frac{\mathrm{Precision}\cdot\mathrm{Recall}}{\left(\sigma^2\cdot\mathrm{Precision}\right)+\mathrm{Recall}} \tag{20}$$

其中，σ 表示精确率的权重，用于调节精确率与召回率的比重，当 $\sigma=1$ 时，称之为F1值。

4.3　对比信任模型

为评估CDNS-TM的性能，本文考虑两项对比信任模型，分别为基于信任的卫星资源切片访问授权机制（BCCTM, beta, communication byte fluctuation, and concentrated trend measurement）[27]与分布式信任评估机制（DTEM, distributed trust evaluation mechanism）[30]。其中，BCCTM考虑三维直接信任（授权信任、忠诚信任、通信信任）与推荐信任，利用多重权重和方法聚合直接信任与间接信任，评估卫星综合信任值，并利用信任阈值评估卫星是否可信。DTEM基于证据理论，根据历史直接交互记录生成信任证据，并计算直接信任，通过权重和聚合直接信任与推荐信任向量，生成聚合信任值，再利用信任阈值判断被评估卫星是否可信。若

被评估卫星为恶意卫星，则评估卫星与恶意卫星断开通信链路，最终完成信任决策。

4.4 实验结果与分析

4.4.1 数据量与恶意卫星比例的影响

本小节通过调整数据量的多少与恶意卫星的比例，探究这两项因素对准确率、精确率、召回率、F值的影响，以综合衡量CDNS-TM的性能。其中，数据量从3.6×10^3个增长至1.8×10^4个。恶意卫星与良性卫星数量的比例从10%增加至90%，其步长为10%。

图4展示了数据量与恶意卫星比例对准确率的影响。随着卫星间数据交互数量的增加，在任何恶意卫星比例情况下，准确率均得到了提升。随着恶意卫星比例的增加，同数据量情况下准确率逐渐下降。值得注意的是，尽管在超过50%恶意卫星比例的高威胁环境中，CDNS-TM的准确率仍高于74.95%（数据量为3.6×10^3），当数据量为1.8×10^4时，准确率高于99.38%。

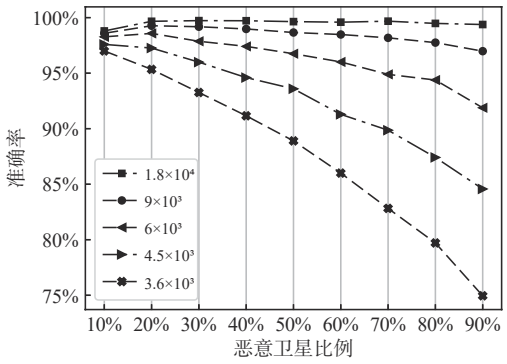


图4　数据量与恶意卫星比例对准确率的影响

图5展示了数据量与恶意卫星比例对精确率的影响。在任意恶意卫星比例场景下，随着数据量的增加，精确率逐步上升。在任意数据量场景下，随着恶意卫星比例的减少，精确率迅速增加，最高达99.62%。当数据量为1.8×10^4时，在极高威胁环境中（90%恶意卫星比例），精确率达94.16%。

图6展示了数据量与恶意卫星比例对召回率的影响。在任意恶意卫星比例场景下，CDNS-TM的召回率高于99.91%，最高达100%，这表明CDNS-TM能够有效识别良性卫星。其次，随着数据量的增加，召回率的波动逐渐降低，趋于稳定。

图7展示了数据量与恶意卫星比例对F1值的影响。数据数量与F1值呈正相关关系，随着数据量的增加，F1值也随之上升，最高达0.998 1。恶意卫星比例与F1值呈负相关关系，随着恶意卫星比

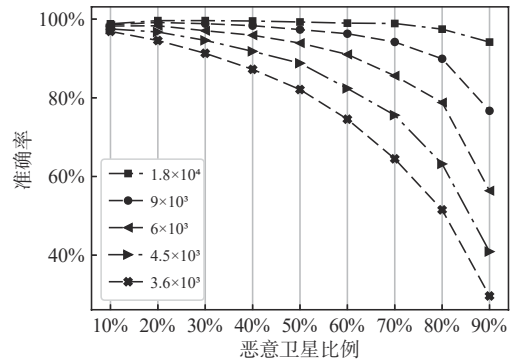


图5　数据量与恶意卫星比例对精确率的影响

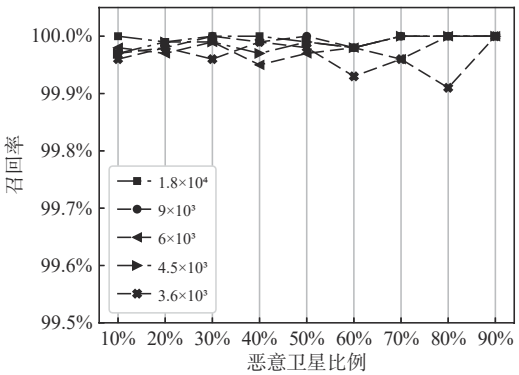


图6　数据量与恶意卫星比例对召回率的影响

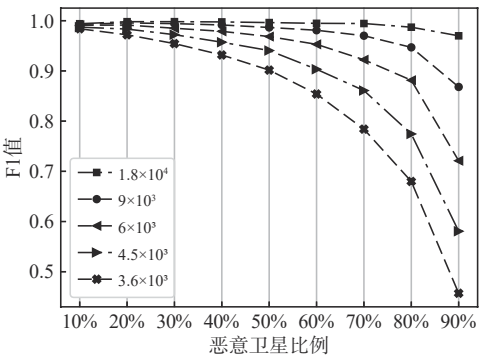


图7　数据量与恶意卫星比例对F1值的影响

例的增加，F1值逐渐降低。当数据量为1.8×10^4、恶意卫星比例为90%时，F1值达到了0.969 9。

适配卫星网络环境的多维度信任评估与聚合是出现上述现象的主要原因。首先，信任观点依赖于数据交互，卫星间数据传输的数量越多，信任观点越可靠。其次，CDNS-TM将卫星星座的整体信任作为参考指标之一，拓展了信任评估维度，为提高识别准确率、精确率、召回率与F1值提供了数据支撑。此外，基于分位图信任观点过滤机制过滤了恶意卫星生成的虚假信任观点，再基于主客观信任聚合方法，综合评估卫星的可靠性，提升了准确率、精确率、召回率与F1值。

4.4.2　不同信任模型的影响

本小节分析了不同信任模型（BCCTM[27]与DTEM[30]）对识别准确率、精确率、召回率与F1值的影响。实验数据量为1.8×10^4，恶意卫星与良性卫星数量的比例从10%增加至90%，其步长为10%。

图8展示了不同信任模型对准确率的影响。CDNS-TM在任意恶意卫星比例的情况下，均保持了极高的识别准确率，其均值为99.52%。尽管BCCTM与DTEM在10%恶意卫星比例场景下的准确率均高于90.15%，但BCCTM与DTEM的准确率随着恶意卫星的比例增加而降低。相比之下，BCCTM比DTEM有更高的准确率。

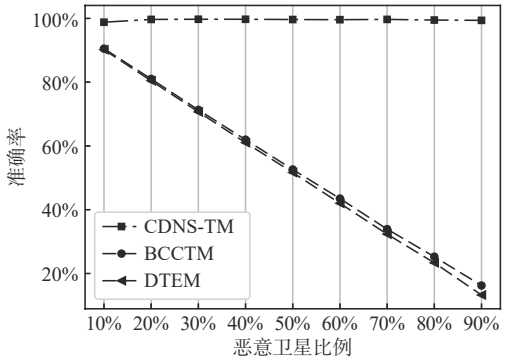


图8　不同信任模型对准确率的影响

图9展示了不同信任模型对精确率的影响。CDNS-TM、BCCTM与DTEM的精确率随着恶意卫星比例的增加而降低。其中，CDNS-TM的精确率受恶意卫星比例的影响较小，在90%恶意卫星比例环境下，精确率达94.16%。BCCTM与DTEM的精确率在高威胁场景中低于50%。

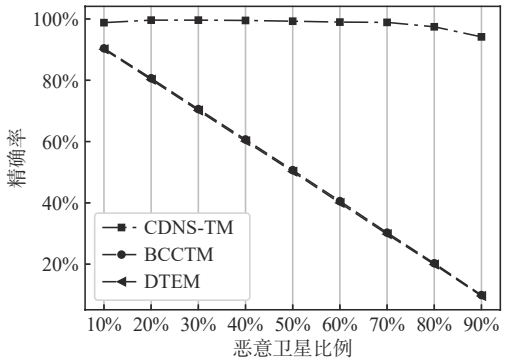


图9　不同信任模型对精确率的影响

图10展示了不同信任模型对召回率的影响。3种信任模型（CDNS-TM、BCCTM与DTEM）在任意恶意卫星比例场景中都保持了较高的召回率，其数值均值分别为99.99%、99.97%与99.96%。其次，上述3种信任模型的方差分别为4.69×10^{-5}、1.94×10^{-5}、4.9×10^{-5}。

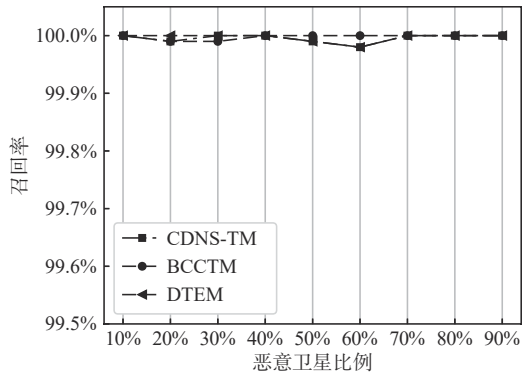


图10　不同信任模型对召回率的影响

图11展示了不同信任模型对F1值的影响。基于精确率与召回率的影响，CDNS-TM的F1值均高于BCCTM与DTEM，其均值为0.992 2。而BCCTM与DTEM的均值分别为0.628 7与0.624 3。其次，随着恶意卫星比例的增加，CDNS-TM、BCCTM与DTEM的F1值逐渐降低，其最低值分别为0.969 9、0.180 5与0.175 5。

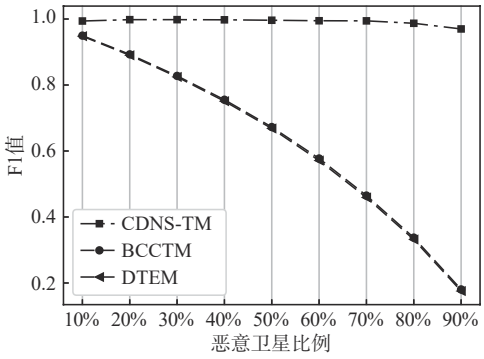


图11　不同信任模型对F1值的影响

造成上述现象的原因，主要体现于以下几个方面。在信任维度方面，CDNS-TM从宏观角度设计了星座信任，以量化集群的整体可信度，使其与微观角度直接信任与推荐信任互补，提供更加准确的评估结果；BCCTM与DTEM仅从微观角度考虑信任影响因素，忽略了宏观层面的集群信任对其信任背书的能力，缺乏多角度的信任评估，或导致信任评估不准确。在信任观点处理方面，BCCTM与DTEM缺乏对虚假信任观点的过滤机制，导致虚假信任观点对信任聚合结果产生负面影响，进而导致信任评估不准确，而CDNS-TM采用分位图过滤机

制量化信任差异，筛除异常信任值，一定程度上增强了信任评估的可靠性。在信任聚合方面，CDNS-TM采用多层信任权重计算方法，根据分位图信任过滤结果，动态计算相邻卫星的权重值，增强了信任观点聚合的准确性；BCCTM与DTEM均采用固定权重聚合信任，难以确保信任聚合的准确性。在机制方面，CDNS-TM设计了自证信任思想与评估方法，通过衡量自证信任与综合信任之间的差异度，判断卫星的可信度，解决了传统信任评估阈值固化问题；BCCTM与DTEM采用固定信任阈值以判断卫星是否可信，而固定阈值存在设置不合理问题，或导致信任评估不准确，难以支撑跨域应用场景。

5　结束语

在卫星互联网场景下，本文提出了一项基于跨域网联态势的多星座信任管理方案。该方案针对多星座场景，考虑多维度信任观点（包括直接信任、推荐信任、星座信任与自证信任等），设计分位图信任过滤机制，过滤潜在异常信任观点，形成信任场与权重场，利用权重和方法聚合信任观点与信任阈值，最终判别出卫星的可信度。实验结果表明，该方案的准确率、精确率、召回率与F值均优于其他基准算法，上述指标均值分别达到了99.16%、96.70%、99.99%与0.982 6。然而，本文所提出的方案依赖卫星间的交互记录，在稀疏网络场景中或交互不足情况下，本方案可能存在评估准确度、精确度不高的问题。由于数据服务需求不同，多星座卫星的网络行为存在差异性，针对卫星的网络行为进行准确的行为画像与细粒度行为识别是当前信任管理技术所面临的重要挑战。在未来工作中，构建可预测的分级信任趋势模型，研究恶意卫星行为并利用其行为促进数据传输是最大化网络容量的关键，可增强卫星互联网在威胁环境中的有效运行能力。

参考文献：

[1] 沈学民, 承楠, 周海波, 等. 空天地一体化网络技术: 探索与展望[J]. 物联网学报, 2020, 4(3): 3-19.
SHEN X M, CHENG N, ZHOU H B , et al. Space-air-ground integrated networks: review and prospect[J]. Chinese Journal on Internet of Things, 2020, 4(3): 3-19.

[2] AL-HRAISHAWI H, CHOUGRANI H, KISSELEFF S, et al. A survey on nongeostationary satellite systems: the communication perspective[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 101-132.

[3] 白卫岗, 盛敏, 杜盼盼. 6G卫星物联网移动性管理: 挑战与关键技术[J]. 物联网学报, 2020, 4(1): 104-110.
BAI W G, SHENG M, DU P P. Mobility management of the 6G satellite IoT: challenges and key techniques[J]. Chinese Journal on Internet of Things, 2020, 4(1): 104-110.

[4] KODHELI O, LAGUNAS E, MATURO N, et al. Satellite communications in the new space era: a survey and future challenges[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 70-109.

[5] LI K X, YOU L, WANG J H, et al. Downlink transmit design for massive MIMO LEO satellite communications[J]. IEEE Transactions on Communications, 2022, 70(2): 1014-1028.

[6] 刘洋, 魏锋, 崔树成, 等. 低轨道卫星通信与物联网应用研究[J]. 物联网学报, 2019, 3(4): 101-108.
LIU Y, WEI F, CUI S C, et al. Research on the application of LEO satellite communication and Internet of Things[J]. Chinese Journal on Internet of Things, 2019, 3(4): 101-108.

[7] CENTENARO M, COSTA C E, GRANELLI F, et al. A survey on technologies, standards and open challenges in satellite IoT[J]. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1693-1720.

[8] 王承祥, 黄杰, 王海明, 等. 面向6G的无线通信信道特性分析与建模[J]. 物联网学报, 2020, 4(1): 19-32.
WANG C X, HUANG J, WANG H M, et al. 6G oriented wireless communication channel characteristics analysis and modeling[J]. Chinese Journal on Internet of Things, 2020, 4(1): 19-32.

[9] HU M L, YANG R H, HU Y, et al. QoS-aware software-defined multicast in LEO satellite networks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(6): 5307-5317.

[10] LIANG H, YANG Z Q, ZHANG G B, et al. Resource allocation for space-air-ground integrated networks: a comprehensive review[J]. Journal of Communications and Information Networks, 2024, 9(1): 1-23.

[11] YU Y, LU Q C, FU Y S. Dynamic trust management for the edge devices in industrial Internet[J]. IEEE Internet of Things Journal, 2024, 11(10): 18410-18420.

[12] ULLAH F, SALAM A, AMIN F, et al. Deep trust: a novel framework for dynamic trust and reputation management in the Internet of Things (IoT)-based networks[J]. IEEE Access, 2024, 12: 87407-87419.

[13] ZHANG S B, LIU A J, HAN C, et al. A network-flows-based satellite handover strategy for LEO satellite networks[J]. IEEE Wireless Communications Letters, 2021, 10(12): 2669-2673.

[14] GUO K F, AN K, ZHANG B N, et al. Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5129-5141.

[15] RUAN Z Q, YANG X, LUO H B, et al. A robust and secure data access scheme for satellite-assisted Internet of Things with content adaptive addressing[J]. IEEE Internet of Things Journal, 2024, 11(8): 13393-13410.

[16] TANG F X, WEN C, LUO L F, et al. Blockchain-based trusted traffic offloading in space-air-ground integrated networks (SAGIN):

a federated reinforcement learning approach[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3501-3516.

[17] DING Y M, ZHAO Y, ZHANG R. A secure routing algorithm based on trust value for micro-nano satellite network[C]//Proceedings of the 2020 2nd International Conference on Information Technology and Computer Application (ITCA). Piscataway: IEEE Press, 2020: 229-235.

[18] LI X F, LI R. A comprehensive review for 4-D trust management in distributed IoT[J]. IEEE Internet of Things Journal, 2023, 10(24): 21738-21762.

[19] LI H, SHI D C, WANG W Z, et al. Secure routing for LEO satellite network survivability[J]. Computer Networks, 2022, 211: 109011.

[20] CAI R Y, JU M Y, YANG L, et al. Research on lightweight secure routing technology based on satellite network[C]//Proceedings of the 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT). Piscataway: IEEE Press, 2020: 42-47.

[21] YU Z F, ZHOU H G, WU Z F. A trust-based secure routing protocol for multi-layered satellite networks[C]//Proceedings of the 2012 IEEE International Conference on Information Science and Technology. Piscataway: IEEE Press, 2012: 313-317.

[22] LI J, XUE K P, LIU J Q, et al. A user-centric handover scheme for ultra-dense LEO satellite networks[J]. IEEE Wireless Communications Letters, 2020, 9(11): 1904-1908.

[23] 宋宇杰, 曹越, 陈诺, 等. 基于信道建模的多层星地融合数据分配策略[J]. 通信学报, 2024, 45(7): 70-83.
SONG Y J, CAO Y, CHEN N, et al. Channel model-based multiple layers satellite-ground integrated data allocation strategy[J]. Journal on Communications, 2024, 45(7): 70-83.

[24] WEI Q, CHEN Y Y, JIA Z Y, et al. Energy-efficient caching and user selection for resource-limited SAGINs in emergency communications[J]. IEEE Transactions on Communications, 2024, PP(99): 1.

[25] HE L J, JIA Z Y, GUO K, et al. Online joint data offloading and power control for space-air-ground integrated networks[J]. IEEE Transactions on Wireless Communications, 2024, 23(12): 18126-18141.

[26] JIA Z Y, CAO Y L, HE L J, et al. NFV-enabled service recovery in space-air-ground integrated networks: a matching game based approach[J]. IEEE Transactions on Network Science and Engineering, 2025, PP(99): 1-14.

[27] GUO C, HU G Y, PAN C L, et al. Authentication for satellite Internet resource slicing access based on trust measurement[J]. IEEE Internet of Things Journal, 2024, 11(12): 21788-21806.

[28] SONG Y J, CAO Y, HOU Y Z, et al. A channel perceiving-based handover management in space-ground integrated information network[J]. IEEE Transactions on Network and Service Management, 2024, 21(1): 882-896.

[29] 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.

[30] LI H, SHI D C, ZHOU R J, et al. Distributed trust evaluation mechanism of LEO satellites for 6G network[C]//Proceedings of the 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). Piscataway: IEEE Press, 2021: 819-824.

[31] LIU Z, YUAN Y H, ZHAO B, et al. Trust assessment under the integrated air-space-ground network environment[J]. Tsinghua Science and Technology, 2023, 28(2): 405-420.

[32] YANG W W, SHI L, LIANG H, et al. Trusted mobile edge computing: DAG blockchain-aided trust management and resource allocation[J]. IEEE Transactions on Wireless Communications, 2024, 23(5): 5006-5018.

[33] XU Q, ZHANG L, QIN X J, et al. A novel machine learning-based trust management against multiple misbehaviors for connected and automated vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(11): 16775-16790.

[34] WANG C L, LIU G H, JIANG T. Malicious node detection in wireless weak-link sensor networks using dynamic trust management[J]. IEEE Transactions on Mobile Computing, 2024, 23(12): 12866-12877.

[35] XIAO Y G, LIU Y B. BayesTrust and VehicleRank: constructing an implicit web of trust in VANET[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2850-2864.

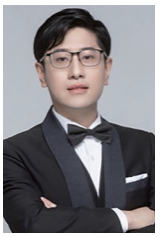
[36] GUMASTE A, NAPOLI A, PEDRO J, et al. Cost-effective IP-over-DWDM aggregation and improved router bypass using P2MP optics[J]. IET Conference Proceedings, 2023, 2023(34): 1059-1062.

[37] KERÄNEN A, OTT J, KÄRKKÄINEN T, et al. The ONE simulator for DTN protocol evaluation[C]//Proceedings of the 2nd International Conference on Simulation Tools and Techniques. New York: ACM Press, 2009: 1-10.

[38] GONG S L, SHEN H, ZHAO K L, et al. Network availability maximization for free-space optical satellite communications[J]. IEEE Wireless Communications Letters, 2020, 9(3): 411-415.

[作者简介]

宋宇杰（1997– ），男，武汉大学国家网络安全学院博士生，主要研究方向为车路协同组网传输、空天地一体化网络信任管理等。



曹越（1984– ），男，博士，武汉大学国家网络安全学院教授，主要研究方向为计算机网络安全、智能交通等。

高骏峤（2000– ），男，武汉大学国家网络安全学院硕士生，主要研究方向为无人机网络信任管理。

赵亮（1984– ），男，博士，沈阳航空航天大学计算机学院教授，主要研究方向为移动计算（车载、无人机、卫星的组网及边缘计算）、智能交通等。

李立（1976– ），男，博士，西北工业大学电子信息学院教授，主要研究方向为先进空天通信与感知等。

孙智立（1961– ），男，博士，萨里大学通信系统研究所教授，主要研究方向为卫星网络与互联网协议等。