联合异常检测的卫星安全传输优化算法

黄 晨,王定轩,侯蓉晖*
(西安电子科技大学网络与信息安全学院,陕西西安 710126)

摘 要: 本文研究卫星网络系统稳定性和安全性问题,为业务提供安全可靠的端到端服务. 针对卫星网络中可能存在的干扰攻击和拒绝服务攻击,考虑异常检测存在错误判断的情况,根据检测误差精度设计联合检测的安全传输方案,最小化端到端时延抖动. 基于最优控制策略构建安全传输优化问题,联合检测需求作为约束条件决策传输路径,利用增广拉格朗日差分进化算法求解得到最优数据传输方案. 首次将异常检测的精确度作为安全传输路径策略的影响因素,当网络中存在一定程度的攻击时,安全控制算法提供稳定的端到端服务,控制策略同时动态触发异常检测,使得网络具备主动防御能力. 本文搭建了66颗卫星星座,分别在卫星网络的干扰攻击和拒绝服务攻击中模拟验证所提出的安全传输方案的有效性. 实验结果表明,将异常检测误差作为安全传输策略的决策因素,可有效提升网络服务的稳定性.

关键词: 卫星网络;主动式攻击检测;干扰攻击;DoS攻击;最优控制
基金项目: 国家自然科学基金(No.U23B2024);中国航天科技集团公司第八研究院产学研合作基金(No.SAST2022-092)
中图分类号: TN927;V474 **文献标识码:** A **文章编号:** 0372-2112(2025)05-1460-09
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240301

Satellite Security Transmission Optimization Algorithm for Joint Anomaly Detection

HUANG Chen, WANG Ding-xuan, HOU Rong-hui*
(*School of Cyber Engineering*, *Xidian University*, *Xi'an*, *Shaanxi* 710126, *China*)

Abstract: This paper studies the stability and security of satellite network system to provide safe and reliable end-to-end service for business. Considering jamming attacks and denial of service (DoS) attacks in the satellite network, a joint detection security transmission scheme is designed according to the detection error accuracy to minimize end-to-end delay jitter. We construct the security transmission optimization problem based on the optimal control strategy, and determine the transmission path by combining the detection requirements as constraints. The optimal data transmission scheme is obtained by the augmented Lagrange differential evolution algorithm. For the first time, the accuracy of anomaly detection is used as a factor to determine the security path policy in this paper. When the network is attacked, the security control algorithm provides stable end-to-end services and the control policy dynamically triggers the anomaly detection, enabling the network to actively defend. In this paper, 66 satellite constellations are constructed to simulate and verify the effectiveness of the proposed secure transmission scheme in jamming attacks and denial of service attacks. The results show that using anomaly detection error as a decision factor of secure transmission strategy can effectively improve the stability of network services.

Key words: satellite network; active attack detection; jamming attack; DoS attack; optimal control
Foundation Item(s): National Natural Science Foundation of China (No.U23B2024); Shanghai Aerospace Eighth Research Institute SAST Foundation (No.SAST2022-092)

1 引言

6G无线网络白皮书提出未来的无线网络需要在地面和空间中联合构建,卫星网络是下一代通信网络的重要组成部分[1]. 新兴的巨型星座(如Starlink[2]、Kuiper[3])具有灵活的网络拓扑和高速互联链路,提供无处不在的高速互联网服务[4]. 另一方面,卫星网络易受信

收稿日期:2024-04-08;修回日期:2024-12-13;责任编辑:李勇锋
*通讯作者:侯蓉晖

号干扰、通信中断、窃听劫持等网络威胁. 文献[5]利用低轨卫星网络的全球可访问性从地面多个位置发动分布式拒绝服务攻击(Distributed Denial of Service, DDoS),根据拓扑通过少量攻击带宽阻碍大面积区域通信. 干扰攻击[6]通过在地面部署干扰源,破坏星地上行控制信号和下行传输信号的接收,阻碍卫星接收地面发送的实时指令.

一般网络路由机制可以分为四个阶段:拓扑结构抽取、路由计算、路由转发和路由维护[7]. 路由转发阶段,也称端到端数据传输阶段,通过综合考虑链路状态、传输需求和风险等因素,为数据包动态选择传输路径. 当前数据安全传输问题日益严峻,在自组织网络[8~10]和卫星网络[11,12]以及其他多种场景有着大量的研究成果. 这些工作通过设置节点信任值区分正常节点和恶意节点,选择信任节点作为下一跳,在一定攻击程度下指导数据包沿着安全路径传输. 常见的信任值计算模型根据节点状态和转发行为构建,但当网络受到严重攻击时,出现故障的节点数量占比增加,仅根据节点信任值无法提供安全端到端传输服务. 因此,现有安全传输算法无法保证在多种攻击下保障数据安全传输.

在系统中部署检测机制成为提升系统鲁棒性的一种解决方案,已广泛应用于无线网络、智能电网[13]和传感器网络[14]. 典型的检测机制根据贝叶斯概率估计攻击概率,识别异常行为. 但异常检测只能检测已知攻击,对检测未知攻击存在局限性. 同时,从检测机制触发到攻击被成功检测存在时间间隔,因此当前异常检测机制无法为系统提供实时防御. 另一方面,控制理论作为一种经典数学理论,借助控制输入解决系统实时优化问题,在高速公路匝道合并[15]、交叉口交通信号控制[16]、无人机缠斗与空地攻击[17]等多种场景广泛使用. 文献[18]中针对信息物理系统(Cyber-Physical Systems, CPS)中阻碍控制器和执行器信息交互的攻击,提出一种基于最优控制的主动式攻击检测方案,通过设计控制输入提升检测性能. 因此,联合检测和控制成为保障系统安全性的新解决思路.

综上所述,本文在数据传输阶段结合检测性能和控制性能联合设计安全传输方案,实现系统主动防御. 本文采用主动式异常检测,及时识别异常节点. 考虑检测误差和检测滞后性,结合动态网络状态和节点历史行为,将异常检测精确度作为选择传输路径的约束条件. 依据满足服务质量(Quality of Service, QoS)的检测目标和控制目标,构建联合优化问题,基于最优控制理论决策传输路径. 同时将路径决策作为检测的触发条件,在开放的网络环境为业务流提供安全传输服务.

2　系统模型与问题描述

2.1　系统模型

在卫星网络中,业务流延迟与传输路径、网络负载和节点性能等因素相关,且延迟的变化主要由系统实时状态导致. 因此,本文选择端到端延迟作为描述动态网络变化的实时指标[19].

信关站 g 与其可见的卫星节点 s_i 构建射频链路,则上行链路[20]的传输速率如式(1)所示:

$$R_g^{s_i}=B\log_2\left(1+\frac{h_p}{B\sigma^2}\right) \tag{1}$$

其中,h 表示信道增益,B 表示带宽,σ^2 表示信道噪声功率密度,p 为地面站所使用的发射功率.

设信关站上传的数据量为 D,则信关站 g 与卫星 s_i 的传输时延[20]如式(2)所示:

$$T_{gs_i}^{\text{trans}}=\frac{D}{R_g^{s_i}} \tag{2}$$

设射频链路的传播速度为 v_d,星地链路的距离 d_{gs_i} 随卫星的运动而变化,则信关站 g 与卫星 s_i 的星地链路传播时延[20]如式(3)所示:

$$T_{gs_i}^{\text{prop}}=\frac{\int_t^{t+\Delta t}d_{gs_i}(t)\,\mathrm{d}t}{\Delta t}\Big/v_d \tag{3}$$

设卫星 s_i 与相邻卫星 s_j 构建星间链路,卫星 s_i 与卫星 s_j 的链路传输速率如式(4)所示[21]:

$$R_{s_i}^{s_j}=\frac{P_tG_{t_s}G_{r_n}L_f^{s_is_j}(t)}{k_bT_s\left(E_b/N_o\right)_rM_a} \tag{4}$$

其中,自由空间损耗如式(5)所示:

$$L_f^{s_is_j}(t)=\left(\frac{c}{4\pi S_{s_is_j}(t)f}\right)^2 \tag{5}$$

其中,P_t 表示信号发射功率,G_{t_s} 和 G_{r_n} 表示发射天线增益和接收天线增益. k_b 和 T_s 表示玻尔兹曼常数和系统噪声温度,$(E_b/N_o)_r$ 表示每比特的能量与噪声功率密度的比值,M_a 表示链路余量. $S_{s_is_j}(t)$ 表示卫星视距,c 和 f 表示光速和频率.

卫星 s_i 与卫星 s_j 星间链路的传输时延[22]如式(6)所示:

$$T_{s_is_{i+1}}^{\text{trans}}=\frac{D}{R_{s_i}^{s_{i+1}}} \tag{6}$$

设卫星缓存区大小为 B_s,处理速率为 S_p,则卫星 s_i 的处理时延[22]如式(7)所示:

$$T_{s_i}^{\text{proc}}=\frac{B_s}{S_p} \tag{7}$$

排队时延取决于节点队列的数据包数量,则卫星 s_i

队列的排队时延[22]如式(8)所示：

$$T=\sum_{s_i\in P^j,s_i\neq s_d}T_{s_i}^{\text{queue}} \tag{8}$$

其中，P^j表示卫星s_i需要执行的多个数据包集合，j表示需要排队的数据包数量，s_d表示目的卫星，$T_{s_i}^{\text{queue}}$表示队列的总排队时延.

因此，端到端时延由传输时延、传播时延、排队时延和处理时延构成，传输总时延[23]如式(9)所示：

$$\begin{aligned}T_{s_i\to s_d}=&\sum_{s_i\in P^j,s_i\neq s_d}T_{s_i}^{\text{trans}}+\sum_{s_i\in P^j,s_i\neq s_d}T_{l_{ij}}^{\text{prop}}\\&+\sum_{s_i\in P^j,s_i\neq s_d}T_{s_i}^{\text{proc}}+\sum_{s_i\in P^j,s_i\neq s_d}T_{s_i}^{\text{queue}}\end{aligned} \tag{9}$$

2.2 问题描述

基于卫星运动的周期性，对整个卫星网络离散化，则系统状态方程建模如式(10)所示：

$$x_{k+1}=\boldsymbol{A}x_k+\boldsymbol{B}u_k \tag{10}$$

其中，矩阵$\boldsymbol{A}$表征系统的固有特征，仅与网络拓扑有关，表征网络拓扑和链路权重，矩阵仅在拓扑变化时才更新. 当拓扑变化，地面中心根据该时间段内收集到的节点、链路和拓扑信息更新矩阵$\boldsymbol{A}$. 同时为了表示时变卫星网络，设置每15 min更新一次矩阵$\boldsymbol{A}$[24].

构建矩阵$\boldsymbol{B}$表征系统实时状况，描述系统被攻击情况. 当节点s_i受到干扰攻击[6]，矩阵$\boldsymbol{B}$对应位置数值不更新，直至节点重新接收到上注信息. 当节点s_i受到DoS攻击[5]，矩阵$\boldsymbol{B}$的第i行对应位置数值无限大，直至节点恢复传输能力. 只有系统安全无攻击，矩阵$\boldsymbol{B}$基于检测模块指导同步更新.

将节点被攻击建模并推广至整个系统，此时状态方程和观测方程见式(11)和式(12)：

$$x_{k+1|\mu}=\boldsymbol{A}x_{k|\mu}+\boldsymbol{B}u_k \tag{11}$$

$$y_{k|\mu}=\boldsymbol{C}x_{k|\mu} \tag{12}$$

其中，$\mu\in\{\mu_1,\mu_2,\cdots,\mu_{2^p}\}$，$p=0,1,\cdots,M$表示节点状态，$M$表示节点数量. 由式(12)可知，系数$\boldsymbol{C}$表征每个端到端服务的观测情况. 上注失败、卫星被干扰、卫星故障和传输链路中断都将造成观测值y的变化.

在网络系统中部署检测单元，使用多模型自适应估计器[25,26]计算后验概率，基于条件概率判断系统状态. 每个状态μ_i，$i=1,2,\cdots,2^p$根据节点s_i自身的健康状态、执行情况和功能属性，按照概率$P(\mu_i)$出现. 基于控制输入u_k，$k=0,1,\cdots,N$，则每个系统状态出现的概率为$P(\mu_i|u_{0:N})$.

为了避免额外的控制输入对系统造成过大影响，则约束条件如式(13)所示：

$$E\left[G_x x_k+G_u u_k\right]\leqslant g,\forall k\geqslant 0,i\in\{1,2,\cdots,2^p\} \tag{13}$$

依据最小化端到端传输时延误差设计本文控制目标，如式(14)所示：

$$\lim_{t\to\infty}e_k=\lim_{t\to\infty}\left(x_k-r_k\right)=0 \tag{14}$$

其中，r_k表示最优状态值.

基于后验概率的成功检测率设计本文检测目标，如式(15)所示：

$$\max P\left(\mu_i|y_{0:N},u_{0:N-1}\right) \tag{15}$$

3 基于开环控制的安全传输机制

3.1 基于开环策略的控制信号

根据系统测量值y和先验概率$P(\mu_i)$，设置当前时间段的控制目标和检测目标，构建联合优化问题确定最优控制信号u^*，基于优化问题选择最优传输路径，保证在时间段$[0,t_N]$内系统检测具有高正确性，同时保证最优控制性能.

3.1.1 控制目标

定义r_k[19]，即在节点状态良好无攻击、链路无故障、网络流量不拥塞，且数据传输决策顺利上注的理想数值，则理想业务服务响应时延T_{best}见式(16)：

$$r_k=T_{\text{best}}=T^{\text{trans}}+T^{\text{prop}}+T^{\text{proc}}+T^{\text{queue}} \tag{16}$$

为了沿着理想安全最优路径传输直至业务流结束，同时减少控制输入成本，则控制目标函数如式(17)所示：

$$J_c\left(u_{0:N-1}\right)=E\left[\sum_{k=0}^{N}\left\|y_k-r_k\right\|_{\boldsymbol{Q}}^2+\sum_{k=0}^{N-1}\left\|u_k\right\|_{\boldsymbol{R}}^2\right] \tag{17}$$

其中，$\boldsymbol{Q}=\boldsymbol{Q}^{\mathrm{T}}\in\mathbb{R}^{m\times m}$是一个正半定矩阵，$\boldsymbol{R}=\boldsymbol{R}^{\mathrm{T}}\in\mathbb{R}^{p\times p}$是一个正定矩阵.

基于文献[18]定理1，式(17)改写为

$$\begin{aligned}J_c(\cdot)=&\sum_{k=0}^{N}\sum_{i=1}^{2^p}P\left(\mu_i\right)u_{0:k-1}^{\mathrm{T}}\boldsymbol{F}_1u_{0:k-1}+\sum_{k=0}^{N-1}u_k^{\mathrm{T}}\boldsymbol{R}u_k\\&+\sum_{k=0}^{N}\sum_{i=1}^{2^p}P\left(\mu_i\right)\boldsymbol{F}_2u_{0:k-1}+\boldsymbol{F}_3\end{aligned} \tag{18}$$

其中，2^p表示系统的状态总数，$\boldsymbol{F}_1$、$\boldsymbol{F}_2$、$\boldsymbol{F}_3$计算式分别见式(19)~式(21)：

$$\boldsymbol{F}_1=\begin{bmatrix}\boldsymbol{B}_{\mu_i}{}^{\mathrm{T}}\left(\boldsymbol{A}^{k-1}\right)^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{A}^{k-1}\boldsymbol{B}_{\mu_i}&\cdots&\boldsymbol{B}_{\mu_i}{}^{\mathrm{T}}\left(\boldsymbol{A}^{k-1}\right)^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{B}_{\mu_i}\\&\cdots&\\(\boldsymbol{B}_{\mu_i})^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{A}^{k-1}\boldsymbol{B}_{\mu_i}&\cdots&(\boldsymbol{B}_{\mu_i})^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{B}_{\mu_i}\end{bmatrix} \tag{19}$$

$$\begin{aligned}\boldsymbol{F}_2=&2\left(\bar{x}_{0|\mu_i}\right)^{\mathrm{T}}\left(\boldsymbol{A}^k\right)^{\mathrm{T}}\boldsymbol{Q}\left[\boldsymbol{A}^{k-1}\boldsymbol{B}_{\mu_i}\boldsymbol{A}^{k-2}\boldsymbol{B}_{\mu_i}\cdots\boldsymbol{B}_{\mu_i}\right]\\&-2r_k^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\left[\boldsymbol{A}^{k-1}\boldsymbol{B}_{\mu_i}\boldsymbol{A}^{k-2}\boldsymbol{B}_{\mu_i}\cdots\boldsymbol{B}_{\mu_i}\right]\end{aligned} \tag{20}$$

$$\begin{aligned}\boldsymbol{F}_3=&\sum_{k=0}^{N}\sum_{i=0}^{2^p}P\left(\mu_i\right)\left(\bar{x}_{0|\mu_i}\right)^{\mathrm{T}}\left(\boldsymbol{A}^k\right)^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{A}^k\bar{x}_{0|\mu_i}\\&+\mathrm{Tr}\left(\boldsymbol{Q}\sum_{k=0}^{N}\sum_{i=1}^{2^p}P\left(\mu_i\right)\boldsymbol{H}_{y,\ (k,\ k)|\mu_i}\right)\\&+\sum_{k=0}^{N}r_k^{\mathrm{T}}\boldsymbol{Q}r_k+\sum_{k=0}^{N}\sum_{i=0}^{2^p}P\left(\mu_i\right)r^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{C}\boldsymbol{A}^k\bar{x}_{0|\mu_i}\end{aligned}\tag{21}$$

其中,系统状态均值$\bar{x}$和系统输出y所对应的协方差矩阵都根据文献[18]计算得到.

3.1.2　检测目标

检测精度表示系统能够准确定位到受害节点的能力,基于当前条件概率尽可能对状态进行正确判断. 在系统中设置N个并行检测单元检测攻击. 检测单元数量N与系统规模有关,不同轨道间至少部署一个检测单元,同轨道间至少部署一个检测单元,基于检测成本、检测性能和检测质量最终确定N的数值.

为了保障系统检测性能,最小化基于后验概率错误识别的概率,则检测目标如式(22)所示:

$$\begin{aligned}J_d(\cdot)=&E\left(\sigma(\hat{\mu})\,|\,u_{0:\,N-1}\right)\\=&\int_{R^{m(N+1)}}\sum_{i=1}^{2^p}\sigma(\hat{\mu})\,P\left(\mu_i\,|\,y_{0:\,N},\,u_{0:\,N-1}\right)\\&\cdot P\left(y_{0:\,N}|u_{0:\,N-1}\right)\mathrm{d}y_{0:\,N}\end{aligned}\tag{22}$$

基于文献[18]定理2,确定式(22)上界为

$$J_d(\cdot)\leqslant\hat{J}_d\left(u_{0:\,N}\right)=\sum_{i+1}^{2^p}\sum_{j=i+1}^{2^p}\sqrt{P\left(\mu_i\right)P\left(\mu_j\right)}\,\mathrm{e}^{-\phi_{ij}}\tag{23}$$

其中,

$$\begin{aligned}\phi_{ij}=&\frac{1}{4}\left(\bar{y}_{0:\,N|\mu_j}-\bar{y}_{0:\,N|\mu_i}\right)^{\mathrm{T}}\left(\boldsymbol{H}_{y|\mu_i}+\boldsymbol{H}_{y|\mu_j}\right)^{-1}\times\left(\bar{y}_{0:\,N|\mu_j}-\bar{y}_{0:\,N|\mu_i}\right)\\&+\frac{1}{2}\ln\left(\frac{\det\left(\dfrac{\boldsymbol{H}_{y|\mu_i}+\boldsymbol{H}_{y|\mu_j}}{2}\right)}{\sqrt{\det\left(\boldsymbol{H}_{y|\mu_i}\right)\det\left(\boldsymbol{H}_{y|\mu_j}\right)}}\right)\end{aligned}\tag{24}$$

每个节点存在0和1两种状态值,则系统总共有512个状态.$[t_1,t_2]$时间段第i个系统状态的先验概率值如式(27)所示:

3.1.3　联合最优问题

综合考虑检测性能和控制性能,结合检测需求和控制需求,构建联合优化问题如式(25)所示:

$$u_{0:\,N-1}^{*}=\begin{cases}\arg\ \min\limits_{u_{0:\,N-1}}\ J_c(\cdot)\,\text{given in}\,(18)\\\text{s.t.}\ \ E\left[G_x x_{k|\mu_i}+G_u u_{k|u_{0:\,k-1}}\right]\leqslant g,\ \ \forall i,\ \forall k\geqslant 0\\J_d(\cdot)\leqslant\hat{J}_d\left(u_{0:\,N}\right)\,\text{given in}\,(23)\end{cases}\tag{25}$$

参照航速优化问题的求解过程[27],本文采用增广拉格朗日优化算法求解联合优化问题,求解式(25)得到时间段$[0,t_N]$的最优控制信号u^*.

3.2　数值示例

基于铱星星座选择3条相邻轨道的9颗相邻卫星构成卫星网络,如图1所示,卫星间均存在星间链路. 在时间段$[t_1,t_2]$内卫星(1,1)为源节点,卫星(3,3)为目的节点,传输路径作为系统状态x,端到端时延作为系统观测值y,其中,x和y服从多项分布,$\boldsymbol{H}_x$和$\boldsymbol{H}_y$由概率密度函数计算.

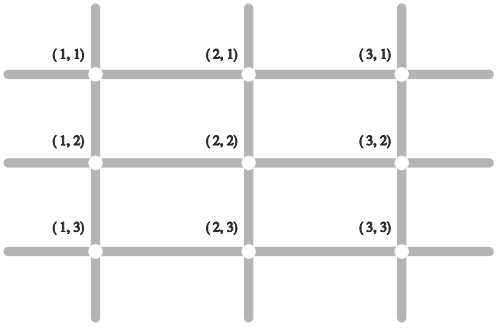


图1　网络规模为3×3的卫星网络示意图

同一轨道上卫星负载相同,各轨道负载分别为2、4、6. 基于节点负载和网络拓扑得到矩阵$\boldsymbol{A}$,矩阵$\boldsymbol{C}$为单位矩阵,t_1时刻系统矩阵$\boldsymbol{B}$如式(26)所示:

$$\begin{bmatrix}4.00&4.00&4.00&8.00&8.00&8.00&12.00&12.00&12.00\\4.00&4.00&4.00&8.00&8.00&8.00&12.00&12.00&12.00\\4.00&4.00&4.00&8.00&8.00&8.00&12.00&12.00&12.00\\8.00&8.00&8.00&16.04&16.04&16.04&24.02&24.02&24.02\\8.00&8.00&8.00&16.04&16.04&16.04&24.02&24.02&24.02\\8.00&8.00&8.00&16.04&16.04&16.04&24.02&24.02&24.02\\12.00&12.00&12.00&24.02&24.02&24.02&36.01&36.01&36.01\\12.00&12.00&12.00&24.02&24.02&24.02&36.01&36.01&36.01\\12.00&12.00&12.00&24.02&24.02&24.02&36.01&36.01&36.01\end{bmatrix}\tag{26}$$

$$P\left(\mu_i\right)=\frac{1}{512},\quad\forall i\tag{27}$$

同轨道星间链路距离为4 033 km,相邻轨道星间链路为3 579 km[24]. 假设每个业务流包含10个

1 000 bits 的数据包，卫星处理效率为 100 KHz，链路传输速率为 1 000 Kbps，则理想情况下端到端时延为 $r_k = 141.894$ ms.

系统模式包含 1、2、512 和 511，其中对应概率如式(28)所示，根据式(18)得到控制目标 J_c.

$$P(\mu_1)=\frac{520}{900},\ P(\mu_2)=\frac{160}{900},P(\mu_{511})=\frac{100}{900},\\ P(\mu_{512})=\frac{120}{900},P(\mu_{i,i\neq 1,2,511,512})=0 \tag{28}$$

假设轨道 1 的状态判断失误概率为 1/27，轨道 2 的失误概率为 1/18，轨道 3 的失误概率为 1/9，则根据式(22)计算检测目标 J_d. 设置检测上界为 $\hat{J}_d=1$，根据式(25)确定控制信号 $u_{0:N-1}$ 的联合优化问题，迭代 30 次得到最优控制信号 u^* 值为 8.4，选择(1, 1)—(1, 2)—(1, 3)—(2, 3)—(3, 3)作为传输路径.

假设下一时间段 $[t_2,t_3]$，干扰攻击影响(1, 3)节点的上注过程，攻击持续 3 s. DoS 攻击发送大量无用数据包攻击(1, 3)节点，攻击持续 2 s. 两种攻击不同时发生.

当系统存在干扰攻击时，此时轨道 1 的失误概率变化为 5/108，轨道 2 为 5/72，轨道 3 为 5/36. 被攻击节点(1, 3)对应位置数据不更新，则矩阵 $\boldsymbol{B}$ 如式(29)所示. 根据式(29)计算得到当前控制最优信号为 $u^*=6.7$. 此时不更改传输路径的选择，选择路径(1, 1)—(1, 2)—(1, 3)—(2, 3)—(3, 3)，在干扰攻击下保证端到端数据安全传输.

当系统存在 DoS 攻击时，如果当前攻击对(1, 3)节点的影响严重，造成节点宕机，则节点直接剔除，则矩阵 $\boldsymbol{B}$ 如式(30)所示. 根据式(30)计算得到 DoS 攻击情况下，当前控制最优信号值为 $u^*=10.2$，在拓扑中剔除(1, 3)节点，则时间段 $[t_2,t_3]$ 最优传输路径更改为(1, 1)—(1, 2)—(2, 2)—(2, 3)—(3, 3).

若当前攻击对(1, 3)节点的影响不严重，仅加剧(1, 3)节点排队情况，不直接剔除(1, 3)节点. 则矩阵 $\boldsymbol{B}$ 如式(31)所示.

$$\begin{bmatrix}
1.00 & 1.00 & 2.00 & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
1.00 & 1.00 & 2.00 & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
2.00 & 2.00 & 4.00 & 8.00 & 8.00 & 6.00 & 12.00 & 12.00 & 10.00\\
4.00 & 4.00 & 8.00 & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
4.00 & 4.00 & 8.00 & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
3.00 & 3.00 & 6.00 & 12.04 & 12.04 & 9.04 & 18.02 & 18.02 & 15.02\\
6.00 & 6.00 & 12.00 & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
6.00 & 6.00 & 12.00 & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
5.00 & 5.00 & 10.00 & 20.02 & 20.02 & 15.02 & 30.01 & 30.01 & 25.01
\end{bmatrix} \tag{29}$$

$$\begin{bmatrix}
1.00 & 1.00 & \infty & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
1.00 & 1.00 & \infty & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
\infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty\\
4.00 & 4.00 & \infty & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
4.00 & 4.00 & \infty & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
3.00 & 3.00 & \infty & 12.04 & 12.04 & 9.04 & 18.02 & 18.02 & 15.02\\
6.00 & 6.00 & \infty & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
6.00 & 6.00 & \infty & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
5.00 & 5.00 & \infty & 20.02 & 20.02 & 15.02 & 30.01 & 30.01 & 25.01
\end{bmatrix} \tag{30}$$

$$\begin{bmatrix}
1.00 & 1.00 & 3.00 & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
1.00 & 1.00 & 3.00 & 4.00 & 4.00 & 3.00 & 6.00 & 6.00 & 5.00\\
3.00 & 3.00 & 9.00 & 12.00 & 12.00 & 9.00 & 18.00 & 18.00 & 15.00\\
4.00 & 4.00 & 12.00 & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
4.00 & 4.00 & 12.00 & 16.04 & 16.04 & 12.04 & 24.02 & 24.02 & 20.02\\
3.00 & 3.00 & 9.00 & 12.04 & 12.04 & 9.04 & 18.02 & 18.02 & 15.02\\
6.00 & 6.00 & 18.00 & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
6.00 & 6.00 & 18.00 & 24.02 & 24.02 & 18.02 & 36.01 & 36.01 & 30.01\\
5.00 & 5.00 & 15.00 & 20.02 & 20.02 & 15.02 & 30.01 & 30.01 & 25.01
\end{bmatrix} \tag{31}$$

根据式(31)计算得到当前控制最优信号为 $u^*=3.1$. 则时间段 $[t_2,t_3]$ 最优传输路径更改为

(1, 1)—(1, 2)—(1, 3)—(2, 3)—(3, 3),在DoS攻击下依然保证端到端数据的安全传输.

4　仿真结果与分析

4.1　仿真设置

本节设置铱星星座包含6条轨道,每条轨道上11颗卫星(包括备份卫星). 地面网络由信关站、地面控制中心和海量终端构成. 根据经纬度设置14个信关站和1个地面控制中心,信关站具体位置如表1所示. 设置$N=7$个检测单元. 基于热门城市人口和经济总量生成流量需求矩阵,根据流量模型得到14个地面站的流量需求矩阵[28,29].

本文利用STK[30]平台实现星座构型,根据TLE网站获取卫星轨道GP信息. 具体卫星网络参数如表2所示. 采用python平台实现完整传输过程,分析14个地面站之间的业务流,模拟多对不同路径长度的业务流[31],具体仿真参数如表3所示.

表1　信关站

地面站	位置(经度,纬度)
Beijing	(116.388, 39.740)
Chengdu	(104.067, 30.498)
Dubai	(55.280, 25.104)
Frankfurt	(8.683, 49.927)
Johannesburg	(28.083, −26.048)
London	(−0.117, 51.312)
Moscow	(37.616, 55.573)
San Francisco	(−122.419, 37.589)
Sao Paulo	(−46.617, −23.393)
Sydney	(151.217, −33.705)
Toronto	(−79.417, 43.474)
Tokyo	(139.751, 35.503)
Shanghai	(121.368, 30.939)
Seattle	(−122.332, 47.415)

表2　低轨卫星网络参数

参数	参数值
轨道数目	6条
每个轨道面上卫星数目/颗	11, 11, 11, 11, 11, 11
卫星节点总数	66个
轨道高度	781 km
轨道倾角	86.4°

4.2　安全传输性能对比

考虑到卫星网络的动态变化和拓扑的可预测性,选择基于DS理论的节点信任值安全算法(SLT算法)[10]和基于可信节点的最优传输算法(D3QN算法)[11]作为对比算法,模拟仿真三种传输方案在不同网络负载下对干扰攻击[6]和DoS攻击[5]的系统端到端服务性能,统计不同网络负载的端到端时延,即传播时延、发送时延、排队时延的总和(暂时忽略处理时延),验证本文所设计协议的安全性和有效性,具体攻击设置如表4所示.

表3　仿真参数设置

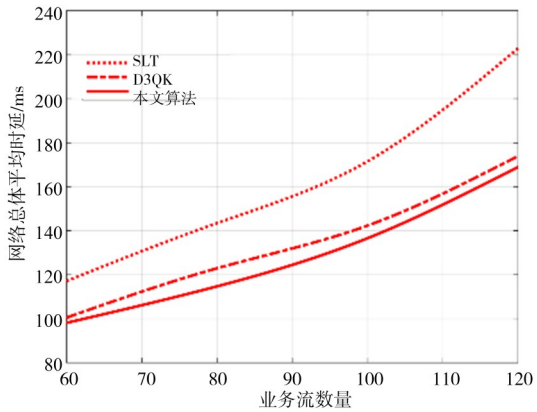
仿真参数	设置值
数据流类型	CBR (Constant Bit Rate)
单个数据流持续时间	15~25 s内的随机值
单个数据包大小	512 Bytes
星间链路带宽	25 MHz
星地链路带宽	14 GHz
数据包最大等待时间	20 ms
仿真运行时间	30 000 ms

表4　攻击参数设置

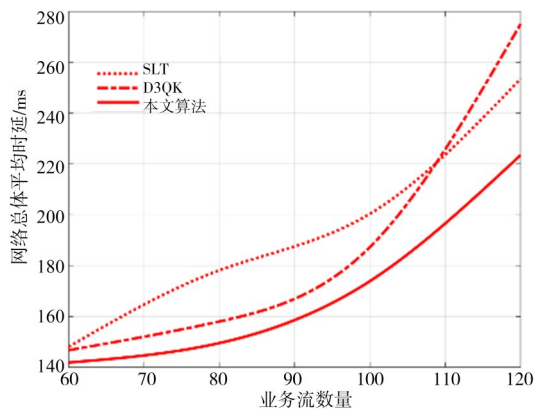
攻击参数	设置值
干扰攻击频率	100 ms/次
干扰攻击间隔	15~25 ms内的随机值
干扰攻击持续时间	3 300 ms
DoS攻击频率	400 ms/次
DoS攻击间隔	15~25 ms内的随机值
DoS攻击持续时间	2 000 ms

三种安全传输方案在不同网络负载下针对干扰攻击和DoS攻击的端到端延迟如图2所示. 横坐标是系统的业务流数量,纵坐标是以ms为单位的端到端延迟. 针对干扰攻击,SLT算法只根据节点行为确定节点信任值,同时SLT不能对攻击主动检测,仅单纯通过信任值衡量节点安全性;D3QN算法除了考虑节点信任值,还根据链路状态联合选择下一跳节点,但D3QN被动判断节点是否受到攻击. 本文所提出的安全传输方案,基于主动检测对干扰攻击进行判断,主动根据当前状态评估节点所受的攻击影响,联合节点安全指标和性能指标选择最优端到端路径. 从图2(a)可知,网络负载较轻时,干扰攻击虽然阻碍数据包的正常接收,但充足的带宽资源为数据传输提供冗余带宽. 然而,在负载较重时带宽资源紧缺,所提出的联合检测安全传输方案考虑了检测精度的误差,有效选择未受干扰攻击的节点,从而保证端到端传输的稳定性.

从图2(b)可知,DoS攻击通过阻塞节点造成链路中断,在成功检测到攻击后选择是否剔除受害节点. 当网络负载较轻时,三种安全传输算法都可以成功避免DoS攻击,为端到端业务选择安全路径. 然而网络负载较重时,节点自身负载状态加重,此时网络中高负载和被攻击节点占比提升,提出的联合检测安全传输方案性能提升比例降低,通过快速识别攻击,保证端到端传输的安全性.



(*a*) 干扰攻击

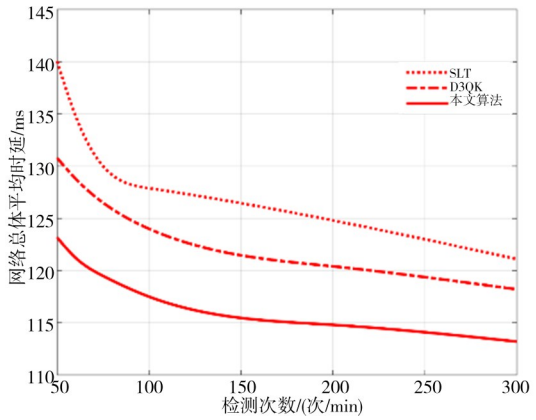


(*b*) DoS攻击

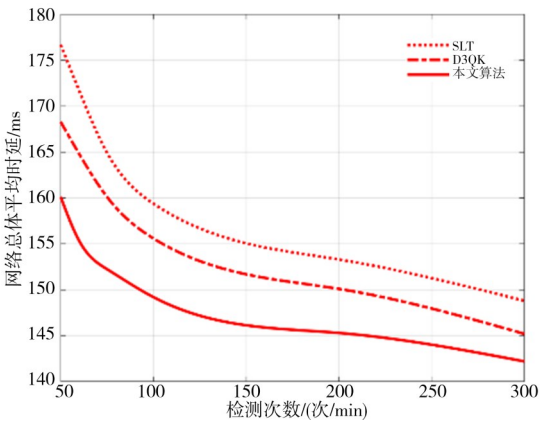
图2 不同网络负载下的系统延迟性能

4.3 检测机制性能对比

在系统中部署检测机制增加系统安全性,对比验证本文所设计的传输算法、SLT算法和D3QN算法的系统性能. 三种安全传输方案在不同检测精度下针对固定系统业务负载量(80业务负载量)的系统性能如图3所示. 检测精度分别为50、100、150、200、250和300次/min. 检测次数越低,检测周期越长,检测精度越小,此时网络中恶意节点被检测的概率越低. 由图3可知,SLT算法和D3QN算法基于固定检测频率,周期性检查系统是否受到干扰攻击和DoS攻击. 当检测精度不高时可能出现节点误判的情况,检测单元误将良好节点剔除,造成系统性能降低. 且仅在攻击出现后触发检测机制,系统不能主动防御. 本文所提出的安全传输方案将检测精度作为路径决策的先验知识,路径决策除了考虑各路径的性能,同时选择节点的历史行为和检测精度作为决策的影响因素,针对干扰攻击和DoS攻击主动触发检测机制,降低检测精度对传输路径安全性的影响. 图3表明,检测精度上升使得系统传输时延性能提升,本文所提出的安全传输方案相比现有方法能进一步优化网络性能.



(*a*) 干扰攻击



(*b*) DoS攻击

图3 不同检测精度下系统延迟性能

5 结论

本文提出一种联合异常检测的卫星网络端到端数据传输控制优化算法. 考虑网络的动态资源状态、DoS攻击和干扰攻击对系统稳定性造成的影响,实时监控网络状态,主动触发攻击检测,保障端到端路径安全. 根据检测精确度指导传输路径决策选择,基于路径决策主动触发检测单元. 基于最小化系统检测误差和最优控制性能分别确定控制目标和检测目标,构建满足系统最低检测精度的联合优化问题,采用进化算法确定最优控制输入. 基于检测精度指导传输路径决策选择安全端到端传输路径. 通过仿真验证了在受到网络攻击的系统中,该控制机制满足系统安全需求并对网络性能稳定具有有效性.

参考文献

[1] CUI J J, NG S X, LIU D, et al. Multiobjective optimization for integrated ground-air-space networks: Current research and future challenges[J]. IEEE Vehicular Technology Magazine, 2021, 16(3):88-98.

[2] SpaceX. Starlink: high-speed, low latency broadband Internet [EB/OL]. (2022-05-12) [2024-03-26]. https://www.starlink.com/.

[3] FCC. Federal Communications Commission FCC 20-102[R/OL]. (2020-09-30) [2024-03-26]. https://docs.fcc.gov/public/attachments/FCC-20-102A1.pdf.

[4] NIEPHAUS C, KRETSCHMER M, GHINEA G. QoS provisioning in converged satellite and terrestrial networks: A survey of the state-of-the-art[J]. IEEE Communications Surveys & Tutorials, 2016, 18(4): 2415-2441.

[5] GIULIARI G, CIUSSANI T, PERRIG A, et al. ICARUS: Attacking low Earth orbit satellite networks[C]//USENIX Annual Technical Conference. California: USENIX Press, 2021: 317-331.

[6] KANTHETI V S R, LIN C H, LIN S C, et al. Anti-jamming resilient LEO satellite swarms[C]//2023 IEEE Military Communications Conference. Piscataway: IEEE Press, 2023: 77-82.

[7] 孙利民, 卢泽新, 吴志美. LEO卫星网络的路由技术[J]. 计算机学报, 2004, 27(5): 659-667.
SUN L M, LU Z X, WU Z M. Routing technology for LEO satellite network[J]. Chinese Journal of Computers, 2004, 27(5): 659-667. (in Chinese)

[8] VELUSAMY D, PUGALENDHI G, RAMASAMY K. A cross-layer trust evaluation protocol for secured routing in communication network of smart grid[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(1): 193-204.

[9] AKTER S, RAHMAN M S, BHUIYAN M Z A, et al. Towards secure communication in CR-VANETs through a trust-based routing protocol[C]//IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE, 2021: 1-6.

[10] FATEMIDOKHT H, RAFSANJANI M K, GUPTA B B, et al. Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7): 4757-4769.

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

[12] SONG J X, JU Y, LIU L, et al. Trustworthy and load-balancing routing scheme for satellite services with multi-agent DRL[C]//IEEE Conference on Computer Communications Workshops. Piscataway: IEEE, 2023: 1-6.

[13] XIE J, RAHMAN A, SUN W. Bayesian GAN-based false data injection attack detection in active distribution grids with DERs[J]. IEEE Transactions on Smart Grid, 2024, 15(3): 3223-3234.

[14] NAHA A, DEY S. Bayesian quickest change-point detection with an energy harvesting sensor and asymptotic analysis[J]. IEEE Transactions on Signal Processing, 2024, 72: 565-579.

[15] SHI Y, WANG Z B, LACLAIR T J, et al. Real-time on-ramp merging control of connected and automated vehicles using pseudospectral convex optimization[C]//2022 American Control Conference (ACC). Piscataway: IEEE, 2022: 2000-2005.

[16] ABBRACCIAVENTO F, ZINNARI F, FORMENTIN S, et al. Real-time optimal traffic management in signal-controlled intersections: A receding-horizon approach[C]//IEEE Conference on Decision and Control (CDC). Piscataway: IEEE, 2021: 1947-1952.

[17] CAO S, WANG X K, YU H C. Real-time maneuver command generation and tracking for a miniature fixed-wing drone with a ducted-fan unit[C]//IEEE Conference on Decision and Control (CDC). Piscataway: IEEE, 2021: 3591-3596.

[18] HOSSEINZADEH M, SINOPOLI B. Active attack detection and control in constrained cyber-physical systems under prevented actuation attack[C]//2021 American Control Conference (ACC). Piscataway: IEEE, 2021: 3242-3247.

[19] TAO B, MASOOD M, GUPTA I, et al. Transmitting, fast and slow: Scheduling satellite traffic through space and time[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2023: 1-15.

[20] 朱琳, 任智源, 国晓博, 等.基于稳态化的卫星网络低时延路由策略[J].无线电通信技术, 2021, 47(5): 603-610.
ZHU L, REN Z Y, GUO X B, et al. Low delay routing strategy based on steady-state satellite network[J]. Radio Communications Technology, 2021, 47(5): 603-610. (in Chinese)

[21] GOLKAR A, LLUCH I CRUZ I. The federated satellite systems paradigm: Concept and business case evaluation[J]. Acta Astronautica, 2015, 111: 230-248.

[22] 徐川, 周密, 赵国锋, 等. 面向确定性传输的新型虚拟卫星编队方案[J]. 通信学报, 2023, 44(10): 137-148.
XU C, ZHOU M, ZHAO G F, et al. A new virtual satellite formation scheme for deterministic transmission[J]. China Industrial Economics, 2023, 44(10): 137-148. (in Chinese)

[23] 王凡, 于啸, 洪涛. 低轨卫星物联网下NB-IoT时延功耗研究[J]. 光通信研究, 2024, 50(3): 123-129.
Research on NB-IoT delay and power consumption in LEO satellite IoT[J]. Study on Optical Communications, 2024, 50(3): 123-129. (in Chinese)

[24] Celestrak. Iridium Current Data[EB/OL]. (2024-09-16)[2024-09-16]. http://www.celestrak.org/.

[25] SADATI N, HOSSEINZADEH M, DUMONT G A. Multi-model robust control of depth of hypnosis[J]. Biomedical Signal Processing and Control, 2018, 40: 443-453.

[26] ROTONDO D, HASSANI V, CRISTOFARO A. A multiple model adaptive architecture for the state estimation in discrete-time uncertain LPV systems[C]//American Control Conference (ACC). Piscataway: IEEE, 2017: 2393-2398.

[27] 张隆辉, 彭秀艳, 魏纳新, 等. 基于增广拉格朗日差分进化算法的长江内河船舶航速优化问题研究[J]. 船舶力学, 2023, 27(8): 1119-1129.
ZHANG L H, PENG X Y, WEI N X, et al. Speed optimization of inland ships on the Yangtze River based on augmented Lagrange differential evolution algorithm[J]. Journal of Ship Mechanics, 2023, 27(8): 1119-1129. (in Chinese)

[28] Socioeconomic Data and Applications Center. Gridded Population of the World (GPW), v4[DB/OL]. (2017-12-01)[2024-05-26]. https://sedac.ciesin.columbia.edu/data/set/gpwv4-population-count-rev11.

[29] LAI Z Q, LI H W, LI J H. StarPerf: Characterizing network performance for emerging mega-constellations[C]//IEEE 28th International Conference on Network Protocols (ICNP). Piscataway: IEEE, 2020: 1-11.

[30] Ansys. Ansys STK software for digital mission engineering and systems analysis[EB/OL]. (2012-07-25)[2024-03-26]. https://www.agi.com/products.

[31] CAO X Y, ZHANG X Y. SaTCP: Link-layer informed TCP adaptation for highly dynamic LEO satellite networks[C]//IEEE Conference on Computer Communications. Piscataway: IEEE, 2023: 1-10.

作者简介

黄 晨 女,1997年6月出生于河南省驻马店市. 现为西安电子科技大学网络与信息安全学院博士研究生. 主要研究方向为卫星网络安全、车联网安全和安全控制.
E-mail: hc5674390@163.com

王定轩 男,2001年8月出生于浙江省江山市. 现为西安电子科技大学网络与信息安全学院硕士研究生. 主要研究方向为卫星网络安全、无人机网络安全.
E-mail: hugh13095820050@163.com

侯蓉晖 女,1980年6月出生于陕西省白水县. 现为西安电子科技大学网络与信息安全学院教授、博士生导师. 主要研究方向为无线组网技术、5G网络、车联网、下一代WLAN系统、卫星组网、网络安全.
E-mail: rhhou@xidian.edu.cn