中国科学:信息科学 2026 年 第 56 卷 第 3 期: 684–703
SCIENTIA SINICA Informationis
中国科学院学部 科学与技术前沿论坛
《中国科学》杂志社
SCIENCE CHINA PRESS
卫星互联网安全专刊 · 论文

基于时序信道预测与展开图神经网络的星间安全空中计算方法

唐晓[1,2], 惠通[3], 杜清河[1], 刘金鑫[4], 张若南[3], 沈超[1*]

1. 西安交通大学电子与信息学部, 西安 710049
2. 西北工业大学深圳研究院, 深圳 518057
3. 西北工业大学电子信息学院, 西安 710072
4. 西安交通大学机械工程学院, 西安 710049
* 通信作者. E-mail: chaoshen@mail.xjtu.edu.cn

收稿日期: 2025–11–19; 修回日期: 2026–01–16; 接受日期: 2026–02–11; 网络出版日期: 2026–02–26

国家自然科学基金 (批准号: 62521002, U22B2013)、广东省基础与应用基础研究基金 (批准号: 2024A1515030215) 和陕西省重点研发计划 (批准号: 2025CG-GJHX-06) 资助项目

摘要 低地球轨道 (low Earth orbit, LEO) 卫星作为 6G 空天地一体化网络的关键支撑, 面临着海量数据高效汇聚与安全保障的双重挑战. 空中计算 (over-the-air computation, AirComp) 利用无线波形叠加实现计算与传输融合, 虽然能显著提升通信和计算效率, 但其无线广播特性使其极易遭受窃听. 针对上述问题, 面向窃听威胁下的高动态星间链路, 解耦信道预测和安全计算决策, 提出一种基于深度学习的安全 AirComp 框架. 首先, 基于卫星轨道动力学先验数据, 建立物理驱动的信道演化模型. 设计基于时序 Transformer 的信道预测网络, 采用残差学习范式, 从历史观测中捕捉信道物理量的非线性演化轨迹, 实现高精度星间信道预测. 在此基础上, 提出基于深度展开图神经网络 (graph neural network, GNN) 的 AirComp 策略求解器, 将迭代优化算法映射为多层展开神经网络, 通过 GNN 中的消息传递建模不同卫星节点间的交互与协同, 高效生成抗窃听的安全 AirComp 波束成形策略. 仿真结果表明, 所提方案在信道参数预测上比传统方法显著降低预测误差, 并且在多种网络配置条件下, 均能实现接近上界的安全 AirComp 速率, 显著优于现有启发式基线 AirComp 方案.

关键词 低地球轨道卫星, 空中计算, 信道预测, 图神经网络, Transformer

1 引言

随着第六代移动通信 (6G) 的空天地一体化网络愿景的逐步落地, 低地球轨道 (low Earth orbit, LEO) 卫星星座正逐渐成为承载全球海量数据的关键基础设施 [1]. 在未来的星群网络中, 卫星不再仅仅是透明的数据管道, 而是通过星间链路紧密互联, 执行包括地球观测、空天感知以及联邦学习等复杂协同计算任务 [2]. 这些任务往往需要在资源受限的星间网络中汇聚并处理海量数据, 对链路带宽与传输效能提出了极高的挑战 [3]. 与此同时, 卫星网络承载的业务数据通常涉及军事侦察、高精测绘或商业机密, 具有极高的敏感性. 因此, 如何在保障传输

引用格式: 唐晓, 惠通, 杜清河, 等. 基于时序信道预测与展开图神经网络的星间安全空中计算方法. 中国科学: 信息科学, 2026, 56: 684–703, doi: 10.1360/SSI-2025-0497
Tang X, Hui T, Du Q H, et al. Secure inter-satellite AirComp with temporal channel prediction and unfolded graph neural network. Sci Sin Inform, 2026, 56: 684–703, doi: 10.1360/SSI-2025-0497

© 2026《中国科学》杂志社 www.scichina.com infocn.scichina.com
https://www.sciengine.com/doi/10.1360/SSI-2025-0497

与计算过程机密性的前提下, 实现星群间大规模数据高效处理, 已成为未来卫星互联网设计中亟待解决的关键问题 [4].

为突破传统通信和计算模式在带宽效率上的瓶颈, 空中计算 (over-the-air computation, AirComp) 作为一种新兴数据处理的范式应运而生 [5]. AirComp 利用无线电磁波在信道中的叠加特性, 支持多个并发节点在同一时频资源块上发送信号, 接收端通过单次观测直接获得目标函数 (如加权和) 的计算结果 [6]. 这种传输即计算的模式摒弃传统的先传输后处理的模式, 将通信时延与带宽消耗从节点数量的线性增长关系降维为常数级, 极大地提升了数据聚合效率 [7]. 在星间通信场景中, 卫星之间的链路通常处于稀疏散射环境, 呈现出显著的视距 (line-of-sight, LoS) 传播特征. 相比于地面的富散射环境, 星间 LoS 信道更加稳定的相位与幅度特性, 为 AirComp 所需的严格信号对齐提供了天然的物理层优势, 为在卫星空间网络中部署 AirComp 提供了巨大的技术潜力 [8].

然而, AirComp 运行所依赖的无线广播环境和对传输信号的精细调控机制, 也使其面临着严峻的安全与隐私威胁 [9]. 在开放的星际空间中, 邻近的非协作卫星或空地节点极易通过旁瓣泄露截获聚合信号, 形成对空中聚合信息的窃取 [10]. 不同于数字加密通信技术, AirComp 的无线信号直接承载了需要聚合的信息, 一旦被窃听者成功解析, 将直接导致聚合结果甚至原始数据的泄露 [11]. 鉴于卫星业务的高敏感性, 需在物理层设计可靠的主动防御机制, 在保证合法接收端聚合精度的同时, 最大程度地混淆窃听者的观测, 从而实现功能安全与信息机密的双重保障 [12].

此外, 星间网络条件下 AirComp 的另一大挑战在于信道的高动态性. LEO 卫星的高速运动导致星间相对几何关系瞬息万变, 信道相干时间较短 [13]. 传统的信道估计 – 资源决策 – 信号传输流程面临严峻的信道老化问题, 传统的优化算法往往需要多次迭代, 难以快速追踪和适配信道状态, 导致收发端的信号预补偿失效, 进而降低 AirComp 的聚合精度或增加窃听风险 [14]. 然而, 星间链路的大尺度衰落、时延、角度演化等主要由轨道动力学决定, 具有高度的可预测性, 而快衰落分量因缺乏多径效应而相对微弱. 这为引入离线训练、在线执行的机器学习信道预测架构提供了物理依据 [15]. 通过深度学习模型从历史观测中挖掘轨道几何的演化规律, 可实现对未来时刻信道状态的高效预测, 从而高效完成 AirComp 收发策略设计 [16].

面向星间高效安全数据处理的愿景, 提出一种基于时序信道预测和深度展开学习的星间安全 AirComp 框架. 对此, 摒弃传统基于瞬时信道信息的被动适应策略, 而采用预测 – 决策的主动规划范式. 首先, 基于卫星轨道动力学的物理先验, 为星间信道的物理量建立时序预测框架; 在此基础上, 将星间网络映射为图结构, 建立深度展开图神经网络架构实现安全波束成形. 本文主要贡献总结如下.

(1) 针对高动态星间高效安全数据处理场景, 建立跨时隙安全 AirComp 系统模型, 综合星间 LoS 信道的物理特性与聚合计算的误差传播机制, 为空间网络的功能安全研究提供了新的视角. 相应建立最大化时间平均安全 AirComp 速率的联合优化问题, 针对问题的非凸性与跨时隙耦合特性, 提出了一种两阶段解耦策略, 将复杂的长期优化分解为信道状态时序预测子问题与单时隙安全 AirComp 波束成形子问题.

(2) 针对星间 AirComp 子问题, 设计了一种基于深度展开 (deep unfolding) 的图神经网络 (graph neural network, GNN) 策略求解器. 基于迭代优化思路展开为多层神经网络, 在每一层中将不同节点间的交互映射为图结构中的信息传递, 以协同星间节点的协作传输, 并通过多层展开更新输出逼近最优的波束成形解.

(3) 针对星间链路几何演化的非线性特征, 设计了一种基于时序 Transformer (temporal Transformer) 的预测网络. 将信道主要物理量的名义值和残差进行分离, 利用 Transformer 的自注意力机制捕捉长时历史观测中的微观非线性依赖, 实现对信道物理量残差的高精度预测, 以有效地重建预测信道.

(4) 对所提的 “预测 – 决策” 学习框架进行的仿真实验, 结果表明, 所提时序 Transformer 能够高精度追踪星间链路的变化, 以此为基础, 所提深度展开图神经网络的架构能够有效提升安全 AirComp 的效能, 显著优于传统信道预测算法及启发式 AirComp 策略.

后文内容组织如下: 第 2 节回顾相关工作; 第 3 和 4 节分别介绍系统模型与问题描述; 第 5 节阐述基于深度展开 GNN 的波束成形策略; 第 6 节介绍基于时序 Transformer 的信道预测架构; 第 7 节提供了仿真结果与性能分析; 最后, 第 8 节总结全文.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

2　相关工作

AirComp 技术利用多址接入信道的传输波形叠加特性实现计算与通信的融合, 近年来被广泛应用于分布式信息融合与机器学习中, 如基于 AirComp 的多模态感知计算 [17] 和联邦学习 [18]. 由于其通信即计算的巨大优势, 现有研究也在不同融合其他新兴技术以增强 AirComp 的性能, 如数字域处理 [19]、智能超表面增强 [20]、空天地网络 [21]. 然而, 由于模拟调制的 AirComp 信号直接暴露了聚合数据的统计特征, 易被恶意用户实现空中窃听, 进而数据安全成为一个严峻的挑战. 作为一种新兴技术, AirComp 安全性方面的工作相对较少. 现有研究工作主要利用了物理层安全思想, 利用收发天线的波束成形以及人工噪声注入来提升 AirComp 的安全性. 如利用多节点协作波束和自适应迫零降低窃听端的聚合精度 [22], 以及超表面增强的人工噪声在保证计算误差约束的同时最大化窃听信道的均方误差 [10]. 然而, 上述工作大多基于地面准静态的衰落信道模型, 较少关注空天网络场景, 且假设信道状态信息在传输周期内保持不变或微小波动. 卫星网络极高的相对运动速度导致信道呈现快速时变特性, 直接应用现有的静态安全机制极易因波束对准失效而导致安全性能退化.

为了缓解高动态环境下的信道信息老化问题, 信道预测技术至关重要. 传统方法主要依赖于自回归等统计模型或卡尔曼滤波来跟踪信道参数 [23,24]. 随着深度学习的发展, 基于循环神经网络及其变体长短期记忆网络 (long short-term memory, LSTM) 的数据驱动方法展现出了优于传统算法的性能, 这些网络能够从历史导频序列中挖掘非线性的时序依赖关系, 实现高效高精度的信道预测 [25]. 然而, 现有的数据驱动预测器通常将信道视为纯随机过程, 未能充分利用卫星通信中轨道动力学的物理先验知识 [26]. 星间链路的大尺度衰落与角度演化实际上由确定性的轨道几何主导, 忽略轨迹信息会导致网络在学习过程中浪费大量参数去拟合已知的物理规律, 限制了对微小随机残差的捕捉能力. 此外, 现有的预测工作往往与后续的资源分配决策解耦, 缺乏面向 AirComp 任务的联合设计.

近年来, 在针对复杂无线资源分配问题的工作中, 基于深度学习的方法因其在线推理的高效性而备受青睐. 其中, 深度展开技术通过将迭代优化算法映射为多层神经网络, 结合了模型驱动的可解释性与数据驱动的拟合能力, 如网络感知 [27]、信道估计 [28]、传输优化 [29] 等. 另一方面, 图神经网络凭借其对非欧数据的强大处理能力, 实现对无线网络的高效建模, 被广泛用于解决分布式功率控制与波束成形等问题 [30,31]. 然而, 现有的 GNN 或深度展开策略大多假设系统具备完美的信道状态信息, 并在此假设下进行确定性优化. 面向实际 LEO 场景中, 需要结合轨道的物理规律实现对信道的高精度预测, 同时借助高效的深度学习方法, 完成对高动态环境下的传输决策. 目前面向卫星场景的安全 AirComp 问题尚未被充分探讨, 更缺乏基于学习机制的高效能方案设计, 相关研究亟待开展.

3　系统模型

3.1　网络拓扑与信道模型

考虑一个互联网卫星系统中包含 I 个 LEO, 记作 $\mathcal{I}=\{1,\ldots,I\}$, LEO 面向同一任务独立完成数据采集 (如针对同一地区的遥感等), 再以 AirComp 的方式把自身结果发送到目标 MEO (medium Earth orbit) 进行聚合. 与此同时, 由于空间传输的开放特性, 系统中存在恶意节点, 如其他卫星或空地终端等, 同样意图获取聚合信号. 考虑存在 1 个合法 MEO 聚合端和 1 个恶意窃听端的情况, 系统旨在增强合法端的聚合精度同时混淆窃听端的接收, 如图 1 所示. 在上述系统中, 第 i 颗 LEO 卫星配置 N_i 根天线, 合法 MEO 聚合卫星配置 N_r 根天线, 窃听者 e 配置 N^e 根天线. 进一步, 考虑星间大量数据的运算需求, 建模 T 个离散时隙内的星间 AirComp, 时隙集合记为 $\mathcal{T}=\{1,\ldots,T\}$. 在单个时隙 $t\in\mathcal{T}$ 内, 假定所有信道保持准静态, 而跨时隙条件下, 信道特性随卫星轨道运动与姿态变化而相应演进.

在空间通信中, 由于 LEO 与 MEO 之间的星间链路传播距离远且处于稀疏散射环境, 信道能量高度集中在视距 (LoS) 路径上. 相应采用纯 LoS 模型来刻画该物理信道, 第 i 颗 LEO 到目标 MEO 聚合端的 $N_r\times N_i$ 维信

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

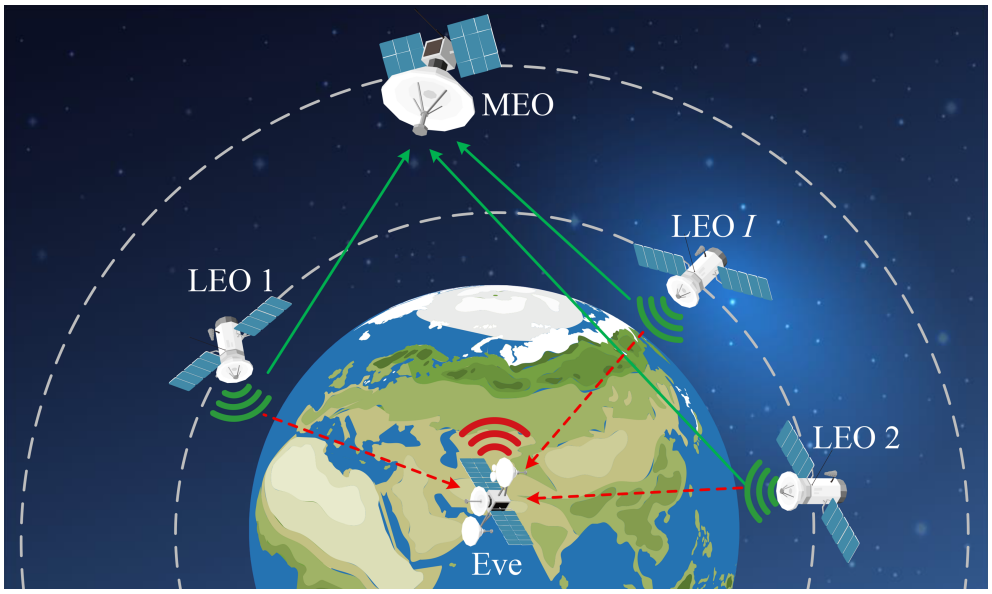


图 1　(网络版彩图) 系统模型.

Figure 1　(Color online) System model.

道矩阵 $\mathbf{H}_i(t)$ 给出为

$$\mathbf{H}_i(t) \triangleq \sqrt{\beta_i(t)}\, \mathbf{a}_r\big(\Omega_{\mathrm{AoA},i}(t)\big)\, \mathbf{a}_i\big(\Omega_{\mathrm{AoD},i}(t)\big)^{\mathsf{H}}\, \mathrm{e}^{-\mathrm{j}2\pi f_c \tau_i(t)}, \tag{1}$$

其中, f_c 为载波频率, $\beta_i(t)$ 是大尺度增益因子, 包含了自由空间路径损耗、收发天线增益等, $\tau_i(t)$ 是由几何距离决定的传播时延, $\Omega_{\mathrm{AoD},i}(t)$ 和 $\Omega_{\mathrm{AoA},i}(t)$ 分别代表 LEO 发射端的离开角和 MEO 接收端的到达角, $\mathbf{a}_i(\cdot)$ 和 $\mathbf{a}_r(\cdot)$ 是 LEO 和 MEO 对应的阵列流形向量. 对于阵列流形向量 $\mathbf{a}(\Omega)$ (Ω 为离开角或到达角), 一般形式如下:

$$\mathbf{a}(\Omega) = \frac{1}{\sqrt{N}}\big[\,\mathrm{e}^{\mathrm{j}k\,\mathbf{p}_1^{\top}\mathbf{u}(\Omega)}, \ldots,\ \mathrm{e}^{\mathrm{j}k\,\mathbf{p}_N^{\top}\mathbf{u}(\Omega)}\,\big]^{\top}, \tag{2}$$

其中波数 $k = 2\pi/\lambda$, 入射或出射方向的单位向量为 $\mathbf{u}(\Omega)$, N 个阵元中第 n 个的相对位置向量为 $\mathbf{p}_n$. 考虑卫星天线多为均匀平面阵, 假设 $N = N_x \times N_y$ (位于 x-y 平面, 间距 d_x, d_y). 若入射波的方位角为 φ、俯仰角为 ϕ, 则 $\mathbf{u}(\Omega) = [\sin\phi\cos\varphi, \sin\phi\sin\varphi, \cos\phi]^{\top}$, 阵列流形可表示为

$$\mathbf{a}(\phi,\varphi) = \mathbf{a}_x(\phi,\varphi) \otimes \mathbf{a}_y(\phi,\varphi), \tag{3}$$

其中

$$\mathbf{a}_x(\phi,\varphi) = \frac{1}{\sqrt{N_x}}[1, \mathrm{e}^{\mathrm{j}kd_x \sin\phi\cos\varphi}, \ldots, \mathrm{e}^{\mathrm{j}kd_x(N_x-1)\sin\phi\cos\varphi}]^{\top}, \tag{4}$$

$$\mathbf{a}_y(\phi,\varphi) = \frac{1}{\sqrt{N_y}}[1, \mathrm{e}^{\mathrm{j}kd_y \sin\phi\sin\varphi}, \ldots, \mathrm{e}^{\mathrm{j}kd_y(N_y-1)\sin\phi\sin\varphi}]^{\top}, \tag{5}$$

相应的参数 N 对应于收发端卫星的天线数 $N_i, \forall i$, N_r.

类似地, 第 i 颗 LEO 到窃听者 e 的 $N^e \times N_i$ 维 MIMO 信道矩阵 $\mathbf{H}_i^e(t)$ 可以表示为

$$\mathbf{H}_i^e(t) \triangleq \sqrt{\beta_i^e(t)}\, \mathbf{a}_r^e\big(\Omega_{\mathrm{AoA},i}^e(t)\big)\, \mathbf{a}_i^e\big(\Omega_{\mathrm{AoD},i}^e(t)\big)^{\mathsf{H}}\, \mathrm{e}^{-\mathrm{j}2\pi f_c \tau_i^e(t)}, \tag{6}$$

其中参数与式 (1) 中的定义一致, 以上标 e 加以区分.

对于星间信道 $\mathbf{H}_i(t)$, $\mathbf{H}_i^e(t)$, $\forall i, t$, 其参数并非完全独立随机变化, 而是强依赖于卫星的轨道动力学和姿态控制, 其中的增益 $\beta_i(t)$、时延 $\tau_i(t)$ 以及角度 $\Omega_{\mathrm{AoD},i}(t)$, $\Omega_{\mathrm{AoA},i}(t)$ 均由 LEO 与 MEO 间的相对几何位置与指向决

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

定, 窃听链路也具有类似的关系. 这些参数随轨道运动呈现出高度平滑和可预测的演化趋势, 因而可以据此完成星间信道预测. 具体地, 将合法信道和窃听信道的物理参量分别提取为

$$\boldsymbol{\theta}_i(t) \triangleq \big[\beta_i(t),\ \tau_i(t),\ \Omega_{\mathrm{AoA},i}(t),\ \Omega_{\mathrm{AoD},i}(t)\big], \quad \boldsymbol{\theta}_i^e(t) \triangleq \big[\beta_i^e(t),\ \tau_i^e(t),\ \Omega_{\mathrm{AoA},i}^e(t),\ \Omega_{\mathrm{AoD},i}^e(t)\big]. \tag{7}$$

通过对信道元素的分离建模, 利用 $\boldsymbol{\theta}_i(t)$ 和 $\boldsymbol{\theta}_i^e(t)$ 中物理量的可预测性进行长期规划, 为安全 AirComp 决策提供依据.

3.2　星间安全 AirComp 模型

在上述系统中, MEO 作为合法聚合端, 在时隙 t 的目标是计算所有 LEO 卫星传输的数据符号 $x_i(t)$ 的加权线性函数, 记作

$$f(t) = \sum_{i\in\mathcal{I}} a_i\, x_i(t), \qquad a_i \in \mathbb{C}, \tag{8}$$

其中 a_i 是第 i 颗 LEO 的数据权重, 数据符号 $x_i(t)$ 零均值, 方差为 $\mathbb{E}[|x_i(t)|^2] = \sigma_i^2$, 且不同 LEO 之间相互独立. 为实现此目标, 第 i 颗 LEO 采用发射波束成形向量 $\mathbf{w}_i(t) \in \mathbb{C}^{N_i\times 1}$, 受限于自身发射功率的约束

$$\|\mathbf{w}_i(t)\|_2^2 \ \leqslant\ P_i, \qquad \forall i \in \mathcal{I},\ t \in \mathcal{T}, \tag{9}$$

其中, P_i 是第 i 颗 LEO 的最大发射功率. MEO 聚合端采用线性合并向量 $\mathbf{r}(t) \in \mathbb{C}^{N_r\times 1}$, 且 $\|\mathbf{r}(t)\|_2 = 1, \forall t \in \mathcal{T}$. 显然, 合法端收发策略 $\mathbf{w}_i(t)$ 和 $\mathbf{r}(t)$ 需要联合优化以实现最佳合并. 为简化符号表示, 综合收发波束向量与信道矩阵, 形成等效信道如下:

$$\tilde{h}_i(t) \ \triangleq\ \mathbf{r}(t)^{\mathsf{H}}\, \mathbf{H}_i\big(\boldsymbol{\theta}_i(t)\big)\, \mathbf{w}_i(t), \tag{10}$$

即第 i 颗 LEO 到 MEO 聚合端的等效信道.

MEO 聚合端接收到的观测 $y(t)$ 为所有 LEO 传输符号经过等效信道后叠加的结果, 给出为

$$y(t) \ =\ \sum_{i\in\mathcal{I}} \tilde{h}_i(t)\, x_i(t) \ +\ n(t), \tag{11}$$

其中 $n(t) \sim \mathcal{CN}(0, \sigma_0^2)$ 是 MEO 接收端的加性高斯白噪声. MEO 聚合端进一步以系数 $\gamma(t) \in \mathbb{C}$ 对 $y(t)$ 进行标量缩放, 得到目标函数的估计值 $\hat{f}(t)$, 即

$$\hat{f}(t) \ =\ \gamma(t)^{-1}\, y(t), \tag{12}$$

其中 $\gamma(t)$ 也称为后处理因子, 用于修正聚合信号 $y(t)$, 使其最优地逼近原始合并目标 $f(t)$.

在开放的无线环境下, 窃听端 e 同样经过星间信道获得聚合信号的窃听版本, 将其自身合并向量记作 $\mathbf{r}^e(t) \in \mathbb{C}^{N_e\times 1}$, 对应窃听端的最优策略来最大化窃听效果. 类似地, 第 i 颗 LEO 到窃听端的等效窃听链路表示为

$$\tilde{h}_i^e(t) \ \triangleq\ \mathbf{r}^e(t)^{\mathsf{H}}\, \mathbf{H}_i^e\big(\boldsymbol{\theta}_i^e(t)\big)\, \mathbf{w}_i(t). \tag{13}$$

在此基础上, 得出窃听端接收到的聚合观测为

$$y^e(t) \ =\ \sum_{i\in\mathcal{I}} \tilde{h}_i^e(t)\, x_i(t) \ +\ n^e(t), \tag{14}$$

其中 $n^e(t) \sim \mathcal{CN}(0, \sigma_0^2)$ 是窃听端的接收噪声. 尽管本系统模型考虑单个窃听端, 但该设定可直接扩展至星间对抗中的多窃听节点场景. 对于多颗敌方卫星合谋窃听的情况, 可将其整体建模为一个拥有分布式天线阵列的等效单窃听端; 对于多颗卫星独立窃听的情况, 系统安全性受限于信道条件最优的窃听节点, 可通过聚合所有潜在威胁的信道特征, 以最大化最差情况下的安全速率. 因此, 本文模型可直接拓展适配存在多个恶意端的工作场景.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

4　问题建模与分解

本节面向前述互联网卫星系统建立安全 AirComp 模型, 其包括两个部分, 一方面是基于历史观测建立多时隙星间链路的预测模型, 另一方面是 LEO 端的发射波束 $\{\mathbf{w}_i(t)\}_{i\in\mathcal{I},t\in\mathcal{T}}$ 和 MEO 端的接收波束 $\{\mathbf{r}(t)\}_{t\in\mathcal{T}}$ 的联合优化设计, 使得 MEO 聚合端的实现高精度计算, 同时尽可能弱化窃听者聚合信息的准确性, 实现跨时隙安全星间 AirComp.

4.1　归一化均方误差

首先, 针对所考虑的星间安全 AirComp 问题建立相应的安全性能度量. 考虑到系统中存在多个聚合端 (MEO 合法端及窃听者), 采用归一化均方误差 (normalized mean square error, NMSE), 作为衡量聚合精度 (合法端) 与信息泄露程度 (窃听端) 的统一尺度. 对于以 MSE 为目标的信号聚合, 可以采用线性最小均方误差估计 (linear minimum MSE, LMMSE) 达到最小的 MSE. 具体来说, 在时隙 t, 目标函数的方差为

$$\sigma_f^2(t) \triangleq \mathrm{var}\big(f(t)\big) = \sum_{i\in\mathcal{I}} |a_i|^2\,\sigma_i^2. \tag{15}$$

合法 MEO 聚合端的标量观测为 $y(t)$, 可以证明, 观测值相对聚合目标 $f(t)$ 的 LMMSE 估计 $\bar{f}(t)=\alpha y(t)$ 所能达到的最小 MSE 为

$$\mathrm{MSE}^{\min}(t) = \sigma_f^2(t) - \frac{|\mathrm{cov}(t)|^2}{\mathrm{var}(t)}, \tag{16}$$

其中协方差 $\mathrm{cov}(t)$ 与方差 $\mathrm{var}(t)$ 定义为

$$\mathrm{cov}(t) \triangleq \mathbb{E}\big[f^*(t)\,y(t)\big], \quad \mathrm{var}(t) \triangleq \mathbb{E}\big[|y(t)|^2\big]. \tag{17}$$

对于上述结论, 可以基于线性估计 $\bar{f}(t)=\alpha y(t)$ 推导对应 MSE, 将其关于尺度因子 α 求一阶导数并将导数置零, 利用所得最优 α 即可得到式 (16) 给出的最小 MSE. 在此基础上, NMSE 定义为最小 MSE 与目标函数自身方差之比, 记作

$$D(t) \triangleq \frac{\mathrm{MSE}^{\min}(t)}{\sigma_f^2(t)} = 1 - \frac{|\mathrm{cov}(t)|^2}{\sigma_f^2(t)\,\mathrm{var}(t)}. \tag{18}$$

易见, $D(t)$ 的取值在 $[0,1]$ 之间, $D(t)\to 0$ 表示合法端的高精度估计, $D(t)\to 1$ 表示完全无法有效聚合信息. 考虑到发送信号 $x_i(t)$ 相互独立、零均值、方差 σ_i^2 的统计特性, 可推出

$$\mathrm{cov}(t) = \mathbb{E}\big[f^*(t)\,y(t)\big] = \sum_{i\in\mathcal{I}} a_i^*\,\tilde{h}_i(t)\,\sigma_i^2, \quad \mathrm{var}(t) = \mathbb{E}\big[|y(t)|^2\big] = \sum_{i\in\mathcal{I}} |\tilde{h}_i(t)|^2\,\sigma_i^2 + \sigma_0^2. \tag{19}$$

带入式 (18) 可得 MEO 合法端的 NMSE 为

$$D(t) = 1 - \frac{\left|\sum_{i\in\mathcal{I}} a_i^*\,\tilde{h}_i(t)\,\sigma_i^2\right|^2}{\sigma_f^2(t)\,\left(\sum_{i\in\mathcal{I}} |\tilde{h}_i(t)|^2\,\sigma_i^2 + \sigma_0^2\right)}. \tag{20}$$

类似地, 窃听端同样基于 LMMSE 估计处理接收信号, 得到 NMSE 为

$$D^e(t) = 1 - \frac{|\mathrm{cov}^e(t)|^2}{\sigma_f^2(t)\,\mathrm{var}^e(t)} = 1 - \frac{\left|\sum_{i\in\mathcal{I}} a_i^*\,\tilde{h}_i^e(t)\,\sigma_i^2\right|^2}{\sigma_f^2(t)\,\left(\sum_{i\in\mathcal{I}} |\tilde{h}_i^e(t)|^2\,\sigma_i^2 + \sigma_0^2\right)}, \tag{21}$$

其中

$$\mathrm{cov}^e(t) = \mathbb{E}\big[f^*(t)\,y^e(t)\big] = \sum_{i\in\mathcal{I}} a_i^*\,\tilde{h}_i^e(t)\,\sigma_i^2, \quad \mathrm{var}^e(t) = \mathbb{E}\big[|y^e(t)|^2\big] = \sum_{i\in\mathcal{I}} |\tilde{h}_i^e(t)|^2\,\sigma_i^2 + \sigma_0^2. \tag{22}$$

与 $D(t)$ 相对应, $D^e(t)\to 0$ 表示聚合信息在窃听端具有高泄露, $D^e(t)\to 1$ 表示窃听端难以完成信息聚合.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

4.2　跨时隙联合优化建模

前述基于 NMSE 为合法端及窃听端建立了信息聚合性能的度量, 其依赖于 LEO 端的发射策略以及接收端的合并策略. 从安全 AirComp 的角度, 需要在功能精度和安全防护的取得平衡. 基于相关文献中 AirComp 速率的定义, 以合法端和窃听端的 AirComp 加权速率差作为系统安全性能的度量, 即私密 AirComp 速率, 在时隙 t 给出为

$$J_t \triangleq \log\frac{1}{D(t)} - \mu\log\frac{1}{D_e(t)}, \tag{23}$$

其中 $\mu\in[0,1]$ 为权重因子, log(1/MSE) 即 AirComp 速率, 单位为 num/Hz, 最大化 J_t 也即旨在增大窃听失真 $D_e(t)$ 与合法失真 $D(t)$ 之间的差距, 体现安全性保障. 类比于物理层安全中私密速率的概念, 上述安全指标用以评估合法端和窃听端共存条件下的 AirComp 私密性.

在单时隙星间安全 AirComp 的基础上, 系统在 T 个时隙上的全局性能定义为

$$\bar{J} = \frac{1}{T}\sum_{t=1}^{T} J_t, \tag{24}$$

即跨多时隙的总体安全性能. 将每时隙的合法端决策变量集合记作 $\mathcal{U}(t) \triangleq \left\{\mathbf{r}(t), \{\mathbf{w}_i(t)\}_{i\in\mathcal{I}}\right\}$, 相应的跨时隙星间安全 AirComp 的联合优化问题可表示为

$$\max_{\{\mathcal{U}(t)\}_{t\in\mathcal{T}}} \quad \frac{1}{T}\sum_{t\in\mathcal{T}} J_t(\mathcal{U}(t), \mathbf{r}^e(t);\ \{\boldsymbol{\theta}_i(t), \boldsymbol{\theta}_i^e(t)\}) \tag{25a}$$

$$\text{s.t.} \quad \|\mathbf{w}_i(t)\|_2^2 \leqslant P_i, \quad \forall i\in\mathcal{I}, \quad \forall t\in\mathcal{T}, \tag{25b}$$

$$\|\mathbf{r}(t)\|_2 = 1, \quad \forall t\in\mathcal{T}, \tag{25c}$$

$$\mathbf{r}^e(t) = \mathbf{r}^{e,\star}\left(\{\mathbf{w}_i(t)\}_{i\in\mathcal{I}}\right), \quad \forall t\in\mathcal{T}, \tag{25d}$$

其中目标函数不仅取决于收发波束, 也依赖于对 T 个时隙内的信道感知和预测情况, 同时假定窃听者也采用最优合并策略 (25d) 来最小化其 $D_e(t)$. 易见, 上述优化问题非常复杂难以求解, 其目标函数关于优化变量高度非凸, 且需要考虑跨时隙的信道预测及对未来的影响.

4.3　预测与决策的问题分解

考虑到问题 (25) 复杂非凸, 直接求解非常复杂. 相应对问题进行分解, 以实现高效的算法设计. 通过对原问题的观察易见, 在信道状态给定的情况下, 每个时隙的星间安全 AirComp 可遵循相同的算法, 而跨时隙的星间链路预测不依赖于 AirComp 的策略. 因此, 将优化问题 (25) 分解为两个子问题, 一方面是基于历史信息的信道预测, 另一方面是时隙化的安全 AirComp 策略. 整体求解框架如图 2 所示, 具体介绍如下.

对于时序化信道预测子问题, 其利用历史观测对当前时隙 t 的信道状态物理量进行预测. 利用卫星轨道及姿态传播器得到信道物理量的名义值, 再基于数据驱动模型预测其残差, 进而重建出预测的星间信道. 对于时隙化 AirComp 策略子问题, 其基于当前时隙的预测信道, 给出合法端的 AirComp 策略, 实现最大化的星间 AirComp 的安全指标 $J_t, \forall t\in\mathcal{T}$.

在实际运行中, 采用在线滚动执行的方案, 即在任意时隙 t 开始时, 利用 $t-1$ 时刻及之前的历史观测, 更新时序预测器, 得到当前时隙 t 的信道. 求解本时隙内的 AirComp 优化问题, 得到优化的收发波束. 执行本时隙的 AirComp 策略, 同时采集新的观测数据 (如导频、几何), 用于更新信道历史序列. 重复以上步骤, 完成跨时隙的星间安全 AirComp. 易见, 由于星间链路的高速快变特性, 信道预测和 AirComp 决策都需要高效地进行, 以适配星间通信环境实现在线决策.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

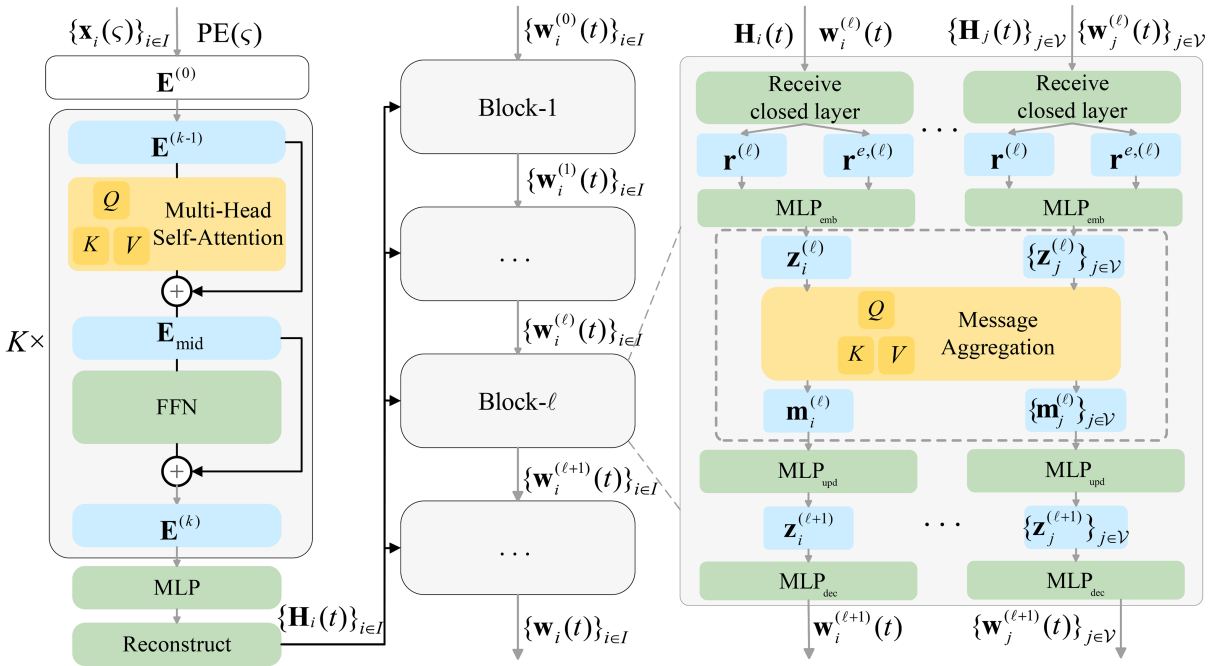


图 2　(网络版彩图) “预测 – 决策” 求解框架 (基于时序 Transformer 的预测与基于深度展开 GNN 的 AirComp 决策).

Figure 2　(Color online) The “prediction-decision” framework (temporal Transformer for channel prediction and unfoled GNN for AirComp strategy).

5　基于深度展开 GNN 的安全 AirComp 策略

考虑单个时隙内星间安全 AirComp 的策略子问题, 其求解也面临高度非凸性的挑战. 由于卫星的高速运动, 星间链路状态变化剧烈, 传统的优化算法虽然也可以求解和收敛, 但通常需要较多轮次的迭代, 难以适配 LEO 动态场景下的快速决策需求. 为此采用基于深度学习的策略设计, 考虑到纯粹黑盒的方法 (如基于 MLP 的信道到策略的拟合) 可解释性较差, 也无法充分利用网络的结构性信息, 以 GNN 为基础建立深度展开框架来设计解决方案.

提出的深度展开框架融合模型驱动与数据驱动方法, 其基本思想是将传统交替优化 AirComp 求解算法的迭代过程映射为一个展开的神经网络, 在这个展开的结构中, 对于易于求解的部分, 保留其显式计算; 对于难以求解的部分, 采用 GNN 模块来拟合该优化步骤. 使用 GNN 的动机是, LEO 节点和不同接收端天然形成了图结构, GNN 的消息传递机制能够有效追踪和学习 LEO 之间的干扰与协作关系, 以实现全局信息聚合目标的优化.

5.1　图构建

建立从星间拓扑的图结构映射是 GNN 学习模型的基础. 采用仅针对 LEO 发射端建图的思路, 相应接收端基于最优响应嵌入到展开结构中, 也即在图结构中仅显式表达 LEO 发射端. 这种设计的内在逻辑是, 在 AirComp 的机制下, 由发射端主动决策而接收端被动响应, 因而接收端策略可以看作是发射波束的函数, 可以认为只有发射策略是实质上的优化变量. 此外, 这样的设计能够最大程度上简化图结构, 提升对不同网络状态变化的泛化能力. 考虑到本小节处理单时隙下的策略, 省略时隙指示 $t \in \mathcal{T}$, 所有决策基于当前时隙的信道预测.

面向星间安全空中计算网络, 以 LEO 节点为基础建立协作图, 图中节点和边的定义如下给出. 节点 (vertex): 图的节点集 $\mathcal{V}$ 与 LEO 卫星集合 $\mathcal{I}$ 对应, 每个节点 $i \in \mathcal{V}$ 代表第 i 颗 LEO 卫星. 边 (edge): 在 AirComp 场景中, 任意 LEO 的发射信号都会同时影响合法 MEO 接收端和窃听者 e 接收端的信噪比. 不同 LEO 发射端的协调形成了全连接的边映射. 因此构建一个无向完全图, 边集 $\mathcal{E} = \{(i,j) \mid i,j \in \mathcal{V}\}$ 为任意节点间的无向连接. 节点 i 需从所有邻居 $j \in \mathcal{N}(i) = \mathcal{V} \setminus \{i\}$ 接收信息, 完成 GNN 的消息传递, 以协同调整其发射端的传输策略.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

在建立的图结构的基础上, 为图中的元素建立相应的特征 (feature), 用于节点特征表征与迭代更新. 节点特征包含了节点 i 本地的信道状态参数, 以及接收上下文, 记作

$$\mathbf{z}_i^{(0)} = \mathrm{MLP}_{\mathrm{emb}}\left[\boldsymbol{\theta}_i, \boldsymbol{\theta}_i^e, \boldsymbol{s}_i^{(0)}\right], \tag{26}$$

其中上标 0 代表初始化层, $\boldsymbol{\theta}_i$ 和 $\boldsymbol{\theta}_i^e$ 代表了当前对节点 i 相关信道物理量的预测值, 其中的角度信息经过正弦编码以去除 2π 模糊性, $\boldsymbol{s}^{(0)}$ 代表接收上下文, 初始化为零向量. 图中的边仅用作节点在 GNN 中的消息传递路径, 因而无需定义边的特征.

5.2　深度展开图迭代更新

在建立网络图映射的基础上, 提出的深度展开 GNN 基于 L 层 ($\ell = 1, \ldots, L$) 迭代模块构造, 其中每一层均模拟了交替优化的迭代轮次, 即首先固定发射端 $\{\mathbf{w}_i\}_{i\in\mathcal{I}}$ 求解最优接收端 $\{\mathbf{r}, \mathbf{r}^e\}$, 然后固定接收端求解最优发射端. 在此过程中, 接收端策略可以基于解析方式获得闭式表达, 而发射波束的交互相对复杂, 通过基于 GNN 的消息传递与解码获得.

5.2.1　基于 LMMSE 的闭式接收策略

由于 AirComp 问题的特性, 接收策略可以分析推导解析表达, 进而大大简化了深度展开网络中的学习和迭代. 下述 AirComp 分析过程不限于所在的展开层次, 故暂且省略 $\ell \in \mathcal{L}$. 前述推导的合法端和窃听端的聚合性能指标, 即 $D(t)$ 和 $D^e(t)$, 基于接收端的 LMMSE 估计得到. 相应的最小 MSE, 即式 (20) 和 (21), 与接收波束的幅度无关, 因此仅需分析接收端波束的方向.

对于合法 MEO 端, 给定 LEO 发射波束, MEO 端的优化目标是选择 $\mathbf{r}$ 以最小化其 NMSE. 为简化符号表示, 引入

$$\mathbf{u} \triangleq \sum_{i\in\mathcal{I}} \sigma_i^2 a_i^* \, \mathbf{H}_i \mathbf{w}_i, \quad \mathbf{C} \triangleq \sum_{i\in\mathcal{I}} \sigma_i^2 \, \mathbf{H}_i \mathbf{w}_i \mathbf{w}_i^{\mathsf{H}} \mathbf{H}_i^{\mathsf{H}}. \tag{27}$$

最小化接收端 NMSE 等价于最大化式 (20) 中的信噪比项, 即

$$\min_{\mathbf{r}} D \Rightarrow \max_{\mathbf{r}} \frac{|\mathbf{r}^{\mathsf{H}}\mathbf{u}|^2}{\mathbf{r}^{\mathsf{H}}(\mathbf{C} + \sigma_0^2\mathbf{I})\mathbf{r}}. \tag{28}$$

对于上述形如瑞利商最大化的优化问题, 基于 Wiener 合并准则可推导出最优解为

$$\mathbf{r}^\star \propto (\mathbf{C} + \sigma_0^2\mathbf{I})^{-1}\mathbf{u}. \tag{29}$$

类似地, 对于窃听端的最优合并问题, 定义

$$\mathbf{u}^e \triangleq \sum_{i\in\mathcal{I}} \sigma_i^2 a_i^* \, \mathbf{H}_i^e \mathbf{w}_i, \quad \mathbf{C}^e \triangleq \sum_{i\in\mathcal{I}} \sigma_i^2 \, \mathbf{H}_i^e \mathbf{w}_i \mathbf{w}_i^{\mathsf{H}} \mathbf{H}_i^{e,\mathsf{H}}, \tag{30}$$

可得窃听端的最优合并准则为

$$\mathbf{r}^{e,\star} \propto (\mathbf{C}^e + \sigma_0^2\mathbf{I})^{-1}\mathbf{u}^e. \tag{31}$$

5.2.2　GNN 消息传递与解码

在深度展开 GNN 结构中, 每一层展开结构都包含了如下步骤. 首先, 基于当前层的 LEO 发射波束 $\{\mathbf{w}_i^{(\ell)}\}$ 下, 计算合法端 MEO 与窃听者 e 的最优 LMMSE 线性合并向量, 然后基于 GNN 完成图节点间的消息传递和更新, 最后基于 GNN 的输出完成 LEO 发射波束的更新.

在第 ℓ 层, 深度展开过程介绍如下. 首先基于闭式解获得当前层的接收波束, 根据式 (29) 和 (31), 合法 MEO 聚合端和窃听端的接收波束的迭代规则分别给出为

$$\mathbf{r}^{(\ell)} \propto \left(\sum_{i\in\mathcal{I}} \sigma_i^2 \mathbf{H}_i \mathbf{w}_i^{(\ell)} \mathbf{w}_i^{(\ell),\mathsf{H}} \mathbf{H}_i^{\mathsf{H}} + \sigma_0^2\mathbf{I}\right)^{-1} \left(\sum_{i\in\mathcal{I}} \sigma_i^2 a_i^* \, \mathbf{H}_i \mathbf{w}_i^{(\ell)}\right), \tag{32}$$

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

$$\mathbf{r}^{e,(\ell)} \propto \left(\sum_{i\in\mathcal{I}} \sigma_i^2 \mathbf{H}_i^e \mathbf{w}_i^{(\ell)} \mathbf{w}_i^{(\ell),\mathsf{H}} \mathbf{H}_i^{e,\mathsf{H}} + \sigma_0^2 \mathbf{I}\right)^{-1} \left(\sum_{i\in\mathcal{I}} \sigma_i^2 a_i^* \, \mathbf{H}_i^e \mathbf{w}_i^{(\ell)}\right). \tag{33}$$

随后, 把所得接收波束以接收上下文的形式, 嵌入节点的特征中. 接收上下文定义为

$$\mathbf{s}_i^{(\ell)} = \mathrm{MLP}_{\mathrm{ctx}}\Big(\big[\|\widehat{\mathbf{H}}_i^{\mathsf{H}} \mathbf{r}^{(\ell)}\|_2, \|\widehat{\mathbf{H}}_i^{e,\mathsf{H}} \mathbf{r}^{e,(\ell)}\|_2, \sigma_0^2, \mu\big]\Big), \tag{34}$$

其为当前节点给出了前一层中的发射波束与合法 MEO 及窃听端的对齐程度, 为进一步的发射波束调整提供依据. 与节点的初始化特征 (26) 一致, 通过接收上下文, 节点在当前展开层的特征更新为

$$\mathbf{z}_i^{(\ell)} = \mathrm{MLP}_{\mathrm{emb}}\left[\boldsymbol{\theta}_i, \boldsymbol{\theta}_i^e, \boldsymbol{s}_i^{(\ell)}\right], \tag{35}$$

其中已嵌入了节点 i 在前一层的发射波束和当前层的接收波束信息, 以及当前信道的信息.

在建立图节点特征的基础上, 在 GNN 中完成消息传递过程, 即任意节点 i 从邻居节点 $j \in \mathcal{V}\backslash\{i\}$ 接收消息, 并完成自身的消息更新. 在此引入图注意力机制, 首先计算节点间的注意力权重. 对于节点 $i, j \in \mathcal{V}$, 注意力权重为

$$\gamma_{ij}^{(\ell)} = \mathrm{softmax}_{j\in\mathcal{V}\backslash\{i\}}\Big(\boldsymbol{\omega}^\top \sigma\big([\mathbf{W}_q \mathbf{z}_i^{(\ell)} || \mathbf{W}_k \mathbf{z}_j^{(\ell)}]\big)\Big), \tag{36}$$

其中 $\mathbf{W}_q$ 和 $\mathbf{W}_k$ 分别为注意力中的 Query 和 Key 系数矩阵, 与注意力权重向量 $\boldsymbol{\omega}$ 都是可训练的参数, σ 为其中的 LeakyReLU 激活函数. 基于节点间的注意力权重, 生成需要在 GNN 中传递的消息. 从节点 j 到节点 i 的消息给出为

$$\mathbf{m}_{i\leftarrow j}^{(\ell)} = \gamma_{ij}^{(\ell)} \, \mathbf{W}_v \mathbf{z}_j^{(\ell)}, \tag{37}$$

其中 $\mathbf{W}_v$ 是可训练的 value 系数矩阵, 进而在节点 i 得到聚合消息

$$\mathbf{m}_i^{(\ell)} = \sum_{j\in\mathcal{V}\backslash\{i\}} \mathbf{m}_{i\leftarrow j}^{(\ell)}. \tag{38}$$

最终, 各个节点融合自身的当前状态和聚合消息, 得到更新后的节点特征

$$\mathbf{z}_i^{(\ell+1)} = \mathrm{MLP}_{\mathrm{upd}}\Big(\big[\mathbf{z}_i^{(\ell)} \parallel \mathbf{m}_i^{(\ell)}\big]\Big). \tag{39}$$

在上述基于注意力的 GNN 消息传递过程中 $\mathbf{W}_q, \mathbf{W}_k, \mathbf{W}_v, \boldsymbol{\omega}, \mathrm{MLP}_{\mathrm{ctx}}, \mathrm{MLP}_{\mathrm{emb}}, \mathrm{MLP}_{\mathrm{upd}}$ 均为在 L 层之间共享的参数, 以提升模型的泛化性能.

在完成第 ℓ 层的深度展开迭代后, 得到了更新后的节点特征 $\mathbf{z}_i^{(\ell+1)}$, 需要将其重新映射为节点的发射波束. 该步骤可以通过一个 MLP 解码器得到

$$\mathbf{w}_i^{(\ell+1,\mathrm{raw})} = \mathrm{MLP}_{\mathrm{dec}}(\mathbf{z}_i^{(\ell+1)}). \tag{40}$$

最后对合成的波束进行功率投影, 确保其满足最大功率约束

$$\mathbf{w}_i^{(\ell+1)} = \mathbf{w}_i^{(\ell+1,\mathrm{raw})} \frac{\sqrt{P_i}}{\max(\|\mathbf{w}_i^{(\ell+1,\mathrm{raw})}\|_2, \sqrt{P_i})}, \tag{41}$$

$\mathbf{w}_i^{(\ell+1)}$ 即为第 ℓ 层迭代的最终输出, 并作为下一层 $\ell+1$ 闭式接收层的输入, 如此循环 L 次, 完成基于深度展开 GNN 的策略更新.

在上述 GNN 的设计中, 融合了模型驱动和数据驱动的方法, 将接收端可解析的最优线性合并与可行性处理固化为模型驱动模块, 将发射端多节点耦合更新交由展开式图消息传递学习补偿, 从而在固定在线开销下获得更稳定的近似最优策略输出, 同时保持可解释性.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

5.3　模型训练与推理

所提出的深度展开 GNN 策略网络的训练目标是最大化单个时隙的私密 AirComp 速率 (23). 经过 L 层展开后, GNN 的最终输出为 $\mathcal{U}^{(L)}=\{\mathbf{r}^{(L)},\{\mathbf{w}_i^{(L)}\}_{i\in\mathcal{I}}\}$, 其前提条件是当前的信道条件参数 $\boldsymbol{\theta}=[\boldsymbol{\theta}_i,\boldsymbol{\theta}_i^e]_{i\in\mathcal{I}}$. 将深度展开网络参数集合记作 $\boldsymbol{\Psi}$, 在信道条件 $\boldsymbol{\theta}$ 下的策略记作 $\Phi(\boldsymbol{\theta};\boldsymbol{\Psi})$, 则训练过程的损失函数定义为

$$\mathrm{Loss}_{\text{U-GNN}}=-\mathbb{E}_{\boldsymbol{\theta}\sim\boldsymbol{\Theta}}\left\{J_t(\Phi(\boldsymbol{\theta};\boldsymbol{\Psi});\boldsymbol{\theta})\right\},\tag{42}$$

其中 $\boldsymbol{\Theta}$ 是满足要求的信道参数分布.

神经网络的训练过程按如下步骤执行. 首先从信道数据集中采样一个批次, 构建一批信道参数样本. 然后以 LEO 节点为基础构建图映射, 计算初始特征并设置初始波束. 在 L 层深度展开神经网络中, 依次计算接收波束的闭式解, 执行基于注意力的 GNN 消息传递, 并输出更新后的发射波束. 利用输出的收发策略组合计算损失函数, 并基于当前批次的平均完成深度展开 GNN 参数的更新. 在神经网络充分训练之后, 在线执行仅需完成一次前向传播, 即可在当前神经网络参数下, 得出当前时隙星间安全 AirComp 的收发策略.

6　基于时序 Transformer 的星间信道预测

星间 AirComp 策略的有效性高度依赖于对当前信道状态 $\widehat{\mathbf{H}}_i(t)$ 和 $\widehat{\mathbf{H}}_i^e(t)$ 的准确估计. 如前所述, 这些信道矩阵由物理参数 $\boldsymbol{\theta}_i(t)$ 和 $\boldsymbol{\theta}_i^e(t)$ 决定. 这些慢变量由卫星轨道动力学驱动, 随时间平滑演化, 呈现出显著的时间相关性, 因而具有高度可预测性. 为此, 本节旨在设计一个基于时间序列 Transformer 的预测器, 用于从历史观测序列中学习这种复杂的时空演化模式, 并对下一时隙的信道物理参数进行高精度预测. 本文时序预测并非直接采用黑盒网络回归绝对信道, 而是采用名义物理模型与数据驱动残差的混合建模范式. 由轨道几何与链路预算主导的可解析演化趋势构造成名义项, 将传播器误差、姿态抖动、测量噪声等未建模扰动统一归入残差项, 并由时序网络基于历史观测对其进行预测. 通过融合模型驱动与数据驱动方法, 利用物理先验降低学习难度, 提升预测稳定性与泛化鲁棒性.

6.1　残差预测框架

对于合法端, 预测器的目标是估计 t 时刻的信道参数, 即 $\boldsymbol{\theta}_i(t)\triangleq\left[\beta_i(t),\ \tau_i(t),\ \Omega_{\text{AoA},i}(t),\ \Omega_{\text{AoD},i}(t)\right]$, 在星间场景下, 直接预测这些物理量的绝对值具有一定的难度, 因为它们通常具有较大的量值和宽广的动态范围. 为简化学习任务, 采用 “名义值 + 残差” 的预测框架, 即

$$\boldsymbol{\theta}_i(t)=\bar{\boldsymbol{\theta}}_i(t)+\Delta\boldsymbol{\theta}_i(t),\tag{43}$$

其中 $\bar{\boldsymbol{\theta}}_i(t)$ 和 $\Delta\boldsymbol{\theta}_i(t)$ 分别为名义值和残差. 名义值 $\bar{\boldsymbol{\theta}}_i(t)$ 是确定性的, 可由星历和轨道传播模型结合链路预算公式计算得到. 例如, $\bar{\tau}_i(t)$ 来自名义距离与光速的比值, $\bar{\beta}_i(t)$ 来自自由空间路径损耗公式, 相应地, $\bar{\boldsymbol{\theta}}_i(t)$ 构成了信道演化的主体骨架. 残差 $\Delta\boldsymbol{\theta}_i(t)$ 部分是随机的, 包含了轨道传播模型的误差、未建模的卫星姿态抖动、空间扰动效应等, $\Delta\boldsymbol{\theta}_i(t)$ 通常是一个零均值或缓变均值且能量远小于 $\bar{\boldsymbol{\theta}}_i(t)$ 的随机过程.

此处建立的时序 Transformer 的预测目标是, 学习并估计这个难以建模的残差项 $\Delta\boldsymbol{\theta}_i(t)$. 这种做法的优势在于, 网络只需专注于学习低能量、高随机性的残差信号, 而非高动态范围的物理量绝对值, 大大降低了训练难度并提升了预测精度. 同时, 窃听端信道参数的预测也按照相同的方式建模, 此处不再赘述.

为预测 t 时刻的残差 $\widehat{\Delta\boldsymbol{\theta}}_i(t)$, 模型需要输入一段过去 S 个时隙的历史观测序列, 记为 $\{\mathbf{x}_i(\varsigma)\}_{\varsigma=t-S}^{t-1}$. 为了便

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

于实现以及泛化, 选取以下易获取且物理意义显著的量构建特征向量

$$\mathbf{x}_i(\varsigma) = \left[\begin{array}{c} \underbrace{\bar{d}_i(\varsigma)}_{\text{名义距离}}, \quad \underbrace{\dot{\bar{d}}_i(\varsigma)}_{\text{名义径向速度}}, \underbrace{\sin\bar{\phi}_{\mathrm{AoD},i}(\varsigma),\ \cos\bar{\phi}_{\mathrm{AoD},i}(\varsigma),\ \sin\bar{\varphi}_{\mathrm{AoD},i}(\varsigma),\ \cos\bar{\varphi}_{\mathrm{AoD},i}(\varsigma)}_{\text{Tx 俯仰/方位 (名义)}}, \\ \underbrace{\sin\bar{\phi}_{\mathrm{AoA},i}(\varsigma),\ \cos\bar{\phi}_{\mathrm{AoA},i}(\varsigma),\ \sin\bar{\varphi}_{\mathrm{AoA},i}(\varsigma),\ \cos\bar{\varphi}_{\mathrm{AoA},i}(\varsigma)}_{\text{Rx 俯仰/方位 (名义)}}, \underbrace{\log\bar{\beta}_i(\varsigma)}_{\text{名义链路增益}}, \underbrace{\mathrm{SNR}_i^{\mathrm{pilot}}(\varsigma)}_{\text{导频 SNR 观测}} \end{array} \right]^{\top}, \tag{44}$$

其中角度信息进行正弦编码以避免 2π 跳变, 所有实数值在进行 Z-score 标准化后输入神经网络运算. 上述特征向量包含名义值部分和观测值部分, 二者的偏差能够有效地体现残差信息. 其中距离、速度、角度等信息根据几何关系和链路传播计算名义值, 基于导频的 SNR 测量反馈则反映了真实的信道.

6.2　时序 Transformer 预测器

考虑到星间链路和拓扑在秒级平滑, 且每个时隙可以做导频校正和基于 GNN 的决策. 采用滚动一步前瞻的方式对星间 AirComp 链路进行预测, 其相比多步预测更加简洁和稳健, 也足以支撑信息聚合多波束决策. 相应地, 预测任务实质上是一个 “序列到向量” (sequence-to-vector) 的回归问题, 即输入长度为 S 的特征序列, 输出当前 t 时刻的单个残差向量 $\widehat{\Delta\boldsymbol{\theta}}_i(t)$. 对于此问题, 采用编码器 – 回归头的 Transformer 架构, 具体介绍如下.

首先, 将输入序列构建为 Transformer 的内部嵌入表示, 将序列中每个时间步的特征进行投影并加上相对时间位置编码

$$\mathbf{e}_i(\varsigma) = \mathrm{MLP}_{\mathrm{in}}(\mathbf{x}_i(\varsigma)) + \mathrm{PE}(\varsigma), \tag{45}$$

其中 $\mathrm{MLP}_{\mathrm{in}}(\cdot)$ 是一个可学习的线性投影层, 用于将特征映射到隐空间, $\mathrm{PE}(\cdot)$ 表示位置编码, 考虑到星间链路特性, 用 Fourier Time2Vec 进行位置编码.

然后, 基于历史观测序列的隐空间映射形成嵌入序列, 送入 K 层 Transformer 编码器, 相应的隐空间嵌入序列为 $\mathbf{E}^{(0)} = [\mathbf{e}_i(t-S), \ldots, \mathbf{e}_i(t-1)]$. 在编码器的每一层中, 都经过多头自注意力、前馈网络以及残差连接, 其输出作为下一层的输入. 其中在第 k 层, $k = 1, \ldots, K$, 多头自注意过程为

$$\mathbf{E}_{\mathrm{mid}} = \mathrm{MHSA}\left(\mathbf{E}^{(k-1)}\right) + \mathbf{E}^{(k-1)}, \tag{46}$$

其中多头自注意力运算 $\mathrm{MHSA}(\cdot)$ 用于捕捉不同时间步之间的依赖关系, 同时加入原始嵌入以保留上一层的信息, 得到的结果再通过层归一化处理, 即 $\mathbf{E}_{\mathrm{mid}} \leftarrow \mathrm{LayerNorm}(\mathbf{E}_{\mathrm{mid}})$, 以稳定数值分布加速训练收敛. 进一步, 每个时间步的特征通过前馈网络进行非线性变换

$$\mathbf{E}^{(k)} = \mathrm{FFN}\left(\mathbf{E}_{\mathrm{mid}}\right) + \mathbf{E}_{\mathrm{mid}}, \tag{47}$$

其中前馈操作 $\mathrm{FFN}(\cdot)$ 通过双线性层实现, 以增强模型的非线性拟合能力, 经过层归一化后作为第 k 层的最终输出, $\mathbf{E}^{(k)} \leftarrow \mathrm{LayerNorm}(\mathbf{E}^{(k)})$, 同时成为下一层的输入.

经过 K 层编码后, 得到了最终的隐藏状态序列 $\mathbf{E}^{(K)}$, 由于是序列到向量任务, 需要对该序列进行池化操作, 以得到一个能代表整个历史的向量. 在此, 可以抽取最后一个时间步 $t-1$ 对应的隐藏状态, 其已通过自注意力机制编码了所有历史信息

$$\mathbf{f}_i = \mathrm{Pool}(\mathbf{E}^{(K)}). \tag{48}$$

通过池化将包含时间维度的信息压缩为一个固定长度的特征, 作为节点 i 链路在当前时刻的整体状态嵌入. 最后, 这个压缩后的上下文向量 $\mathbf{f}_i$ 被送入一个回归器 $\mathrm{MLP}_{\mathrm{out}}$, 以解码出该时刻的残差预测值

$$\Delta\boldsymbol{\theta}_i(t) = \mathrm{MLP}_{\mathrm{out}}(\mathbf{f}_i), \tag{49}$$

其输出 $\Delta\boldsymbol{\theta}_i(t)$ 是一个维度与 $\boldsymbol{\theta}_i(t)$ 匹配的实值向量, 并作用在名义值上得到当前时刻的最终预测, 如式 (43) 所给出.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

考虑到系统中有 I 条合法链路和 I 条窃听链路, 每条链路都有其自身的几何演化. 采用 Siamese 架构, 即所有链路共享同一组时序 Transformer 网络参数. 在 t 时刻, 预测器会并行地将所有链路的历史序列 $\{\mathbf{x}_i(t-S,\ldots,t-1)\}_{i\in\mathcal{I}}$ 和 $\{\mathbf{x}_i^e(t-S,\ldots,t-1)\}_{i\in\mathcal{I}}$ (窃听链路特征) 输入到同一个 Transformer 模型中, 分别得到各链路独立的残差预测 $\{\Delta\boldsymbol{\theta}_i(t)\}_{i\in\mathcal{I}}$ 和 $\{\Delta\boldsymbol{\theta}_i^e(t)\}_{i\in\mathcal{I}}$. 这种设计确保了模型的可扩展性, 并且它学习的是星间链路的通用时序演化物理规律, 而非特定链路间的耦合关系.

6.3　模型训练与执行

上述信道预测的时序 Transformer 在大规模离线数据集上进行监督训练. 该数据集由观测历史和残差真值组合的样本对构成, 即 $\{(\{\mathbf{x}_i(\varsigma)\}_{\varsigma=t-S}^{t-1}),\Delta\boldsymbol{\theta}_i^\circ(t)\}$, 以预测残差与真实残差之间的均方误差为损失函数进行训练

$$\mathrm{Loss}_{\text{Temp-Xfmr}}=\sum_{p\in\{\beta,\tau,\Omega_{\mathrm{AoD}},\Omega_{\mathrm{AoA}}\}}w_p\sum_{i\in\mathcal{I}}\left\|\Delta\boldsymbol{\theta}_{i,p}(t)-\Delta\boldsymbol{\theta}_{i,p}^\circ(t)\right\|_2^2,\tag{50}$$

其中, p 遍历 $\boldsymbol{\theta}$ 的所有分量, w_p 是用于平衡不同物理量纲的损失权重.

综合时序 Transformer 预测器和基于深度展开 GNN 的安全 AirComp 策略网络, 整体滚动预测执行的过程如下. 在每个时隙开始阶段, 系统收集 $t-1$ 时隙的测量反馈并计算 $t-1$ 相关信道物理量的名义值, 组合成 $\mathbf{x}_i(t-1)$, 并更新历史序列缓存. 将该序列输入已训练好的时序 Transformer, 输出 $\Delta\boldsymbol{\theta}_i(t)$. 计算 t 时刻的信道参数名义值 $\bar{\boldsymbol{\theta}}_i(t)$, 进而重构预测的信道参数 $\widehat{\boldsymbol{\theta}}_i(t)=\bar{\boldsymbol{\theta}}_i(t)+\Delta\boldsymbol{\theta}_i(t)$. 基于预测参数构建 AirComp 信道, 并将其代入到训练好的深度展开 GNN 策略网络, 以计算当前时隙 t 的最优波束 $\mathcal{U}^\star(t)$.

7　仿真结果与分析

本节对所提出的安全 AirComp 框架进行性能评估和分析. 发射端 LEO 与合法端 MEO 的距离在 [2500, 6000] km 区间内均匀分布, 窃听者相对合法 MEO 的方位角和俯仰角偏移在 $[5^\circ,20^\circ]$ 区间内均匀分布, 与 LEO 的距离在 $[3000,6500]$ km 区间均匀分布. 系统时间步长 0.1 s, 总时隙 500 个, 卫星方位角和俯仰角在 $[-0.5,0.5]$ deg/s 范围内随机取值的角速度变化. 系统包含 8 个 LEO 卫星, LEO 发射端配置 2×4 面阵天线, MEO 端和窃听端配置 8×16 面阵天线, 发射和接收端天线增益均取 40 dBi. 星间链路的自由空间路径损耗模型为 $32.44+20\log_{10}(f_c)+20\log_{10}\bar{d}_i(\varsigma)$, 其中载频 30 GHz. 最大发射功率为 50 dBW, 噪声功率为 2×10^{-13} W. 安全 AirComp 速率权重因子取 0.8, AirComp 加权和聚合操作中的数据权重均取 1. 时序 Transformer 预测器取特征序列长度为 100, 预测器层数为 4, 自注意力采用 4 注意力头数, 隐藏维度为 256, 前馈网络维度为 512. 数据集包含 50 组随机序列, 每组序列包含 500 个时隙演变, 按 8 : 2 划分为训练集和测试集. 训练采用 Adam 优化器, 学习率为 5×10^{-4}, 共训练 50 轮次. 深度展开 GNN 模型实现单时隙内安全 AirComp 策略的求解, 展开层数为 4, 消息传递层采用 4 注意力头数, 隐藏层维度为 256. 深度展开 GNN 训练采用 Adam 优化器, 学习率为 1×10^{-4}, 共训练 2000 轮次. 仿真参数设定如表 1 所示.

7.1　神经网络训练收敛结果与分析

为了验证所提出的面向星间安全 AirComp 深度学习架构的可行性, 对神经网络的训练收敛行为进行评估. 在所提方案中, 基于时序 Transformer (标记为 Temp. Xfmr.) 的信道预测和基于深度展开 GNN 的 AirComp 策略是两个独立的神经网络, 其分别基于监督学习和非监督学习方法进行训练, 训练的收敛过程分别在图 3 和 4 所给出. 总体上看, 预测网络和策略网络都能够有效地收敛, 但后者需要更多的训练轮次. 这是因为, 预测器本质上是监督回归任务, 在所提时序 Transformer 框架下仅需学习能量较弱的残差分量, 能够以真实值为引导快速锁定最优映射参数. 相比之下, AirComp 策略网络对应无监督的非凸优化, 需要在复杂的空间中搜索最优解, 相比单纯的函数拟合困难得多, 因而需要更长的训练过程来探索和收敛.

图 3 给出了提出的时序 Transformer 预测网络以及与线性预测和长短期记忆网络基线方法的训练损失下降曲线. 从图中可以观察到, 时序 Transformer 表现出显著的收敛速度优势, 仅经过少量轮次的训练, 预测误差即迅

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

表 1　仿真参数.

Table 1　Simulation parameters.

Item	Value
LEO-MEO distance d_i	Uniform in $[2500, 6000]$ km
Eavesdropper angular offsets (w.r.t. MEO)	Uniform in $[5^\circ, 20^\circ]$
LEO-Eve distance d_i^e	Uniform in $[3000, 6500]$ km
Time step Δt	0.1 s
Number of time slots T	500
Angular-rate variation	Uniform in $[-0.5, 0.5]$ deg/s
Number of LEOs I	8
LEO transmit arrays	2×4
MEO/Eve receive arrays	8×16
Transmit/receive antenna gain	40 dBi
Carrier frequency f_c	30 GHz
Max transmit power $P_{\max}$	50 dBW
Noise power σ_0^2	2×10^{-13} W
Secrecy-rate weight μ	0.8
AirComp data weights $\{a_i\}$	1
Number of sequences	50 random sequences
Sequence length	500 time slots per sequence
Train/test split	8 : 2
Feature sequence length S	100
Encoder layers/heads	4/4
Hidden dim/FFN dim	256/512
Optimizer/learning rate	Adam/5×10^{-4}
Training epochs	50
Unfolding layers/heads	4/4
Hidden dim	256
Optimizer/learning rate	Adam/1×10^{-4}
Training epochs	2000

速下降并稳定在极低的水平. 相比之下, LSTM 网络的收敛曲线较为平缓, 需经过更多轮次才能达到较低误差, 而线性预测器不仅收敛最慢, 且在训练初期表现出较大的震荡. 上述结果验证了 Transformer 中的自注意力机制在捕捉卫星信道物理参数的长时序依赖关系方面具有极高的效率, 也验证了所提出的融合名义值与残差预测框架的有效性.

图 4 展示了基于深度展开 GNN 的策略网络在训练过程中的损失函数以及合法端和窃听端 NMSE 的变化情况. 可以看出, 随着训练轮次的增加, 总损失函数呈现快速下降并最终收敛的趋势, 表明网络有效学习到了最大化的目标函数, 即私密 AirComp 速率对应的波束成形策略. 此外, 从不同聚合端的 NMSE 变化轨迹可以清晰地看到一降一升的现象, 即合法端的 NMSE (标记为 Lgt. NMSE) 迅速降低并稳定在较低值, 确保了合法端 AirComp 的计算精度; 与此同时, 窃听者的 NMSE (标记为 Eve. NMSE) 则被逐渐推高并维持在较高水平, 体现了对窃听端的保密性能. 这种 NMSE 反向变化趋势直观地揭示了 GNN 策略的安全机制, 即在保证合法链路质量的同时, 尽量降低窃听效果, 从而最大化窃听者的聚合误差, 构建星间 AirComp 安全保障.

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

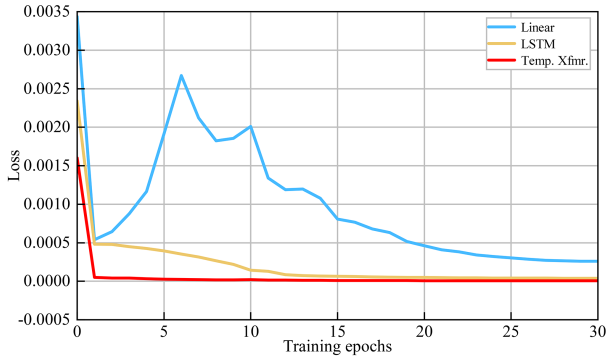


图 3　(网络版彩图) 时序 Transformer 预测器的训练收敛.

Figure 3　(Color online) Convergence of temporal Transformer predictor training.

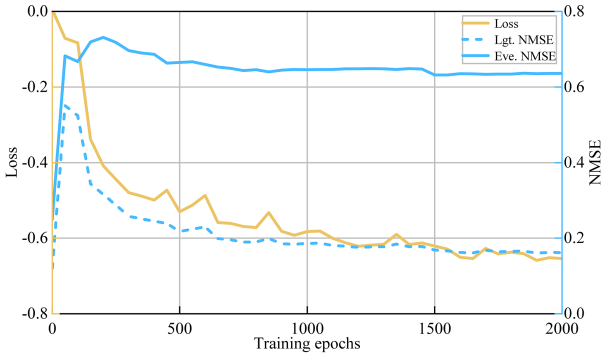


图 4　(网络版彩图) 深度展开 GNN 的训练收敛.

Figure 4　(Color online) Convergence of unfoled GNN training.

7.2　时序 Transformer 预测器结果与分析

为了评估提出的时序 Transformer 预测器的有效性, 将其与两种经典的基线方案进行了对比, 即线性预测器 [23] 和长短期记忆网络 [25]. 其中, 线性预测器假设参数在滑动窗口内呈线性趋势, 适用于短时平滑场景, 但难以捕捉非线性动态; 长短期记忆网络是经典的循环神经网络, 能够建模通用时序依赖. 仿真基于长度 100 的历史序列, 在 200 个连续时隙的滑动窗口上进行单步预测. 此外, 考虑到传播时延与大尺度增益均由星间几何距离决定, 两者具有高度的强相关性与相似的演化规律, 因此主要通过分析信道增益与角度参数来展示预测性能, 不再单独列出时延结果.

图 5 展示了信道大尺度增益的预测轨迹 (上方子图) 与预测误差 (下方子图). 在实验的 LEO 短时窗口内, 链路增益真值呈现出缓慢且平滑的单调变化趋势, 所有评估方案都能追踪到这一变化趋势. 这种平滑性源于星间链路的大尺度衰落主要由自由空间路径损耗决定, 由于 LEO-MEO 绝对距离值大, 在短时观测窗口内, 相对距离变化率较小. 结合误差子图中可以看到, 线性预测器虽然能够跟踪大致趋势, 但其预测误差始终存在显著的偏移与波动, 难以精准拟合轨迹的微小曲率. 长短期记忆网络方法在此类高精度连续值回归任务中表现出相对明显的随机偏移. 相比之下, 所提时序 Transformer 方案得益于 “名义值 + 残差” 的学习框架, 能够将注意力集中在微小的非线性残差上, 从而将预测误差稳定地压缩至最低水平. 这种极高精度的增益估计对于 AirComp 系统至关重要, 它确保了发射端能够精确地执行功率预补偿, 从而严格满足信号在聚合节点的叠加条件.

图 6 和 7 综合展示了发射端方位角与俯仰角的预测性能. 在仿真选定的轨道几何下, 角度参数呈现出准线性演化特征, 但仍包含由轨道投影引起的微小非线性曲率. 这种平滑特性使得线性预测器也能取得可接受的性能, 但其残留误差仍然相对较大. 同时, 长短期记忆网络虽然具备非线性建模能力, 但在本场景中表现出一定的随机振荡, 其预测误差曲线呈现出明显波动特征, 且整体精度甚至在某些时刻劣于线性预测. 其主要原因在于长短时记忆网络试图直接从原始观测序列中学习完整的物理演化规律. 在缺乏名义值作为先验引导的情况下, 难以在较大的数值动态范围中提取出微小轨道动力学特征, 导致输出轨迹缺乏平滑性. 相比之下, 所提的时序 Transformer 能够敏锐捕捉到轨道动力学中由高阶项引起的微小非线性偏离, 将角度预测误差进一步降低. 这证明了所提方案不仅能适应大尺度的轨道运动, 也能胜任星间窄波束通信对指向精度的极致要求.

7.3　星间安全 AirComp 结果与分析

为了综合验证所提时序预测/深度展开学习框架在星间安全 AirComp 中的有效性, 所提方案 (标记为 Temp. Xfmr., U-GNN) 与多组基线方案进行了全面的性能对比. 基线方案包括: 上界基准 (标记为 Perf. info., U-GNN), 即假设已知完美信道状态信息并采用相同的展开 GNN 策略, 用于评估预测误差带来的性能损失; 预测基线方案 (标记为 LSTM, U-GNN), 采用长短期记忆网络替代时序 Transformer 进行信道预测, 用于验证时序模型的

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

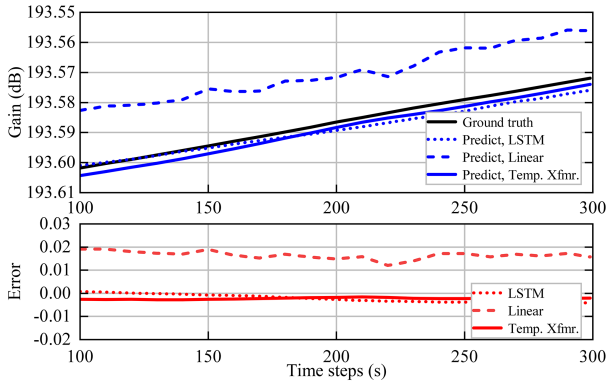


图 5　(网络版彩图) 星间链路增益的预测.

Figure 5　(Color online) Prediction of the satellite channel gain.

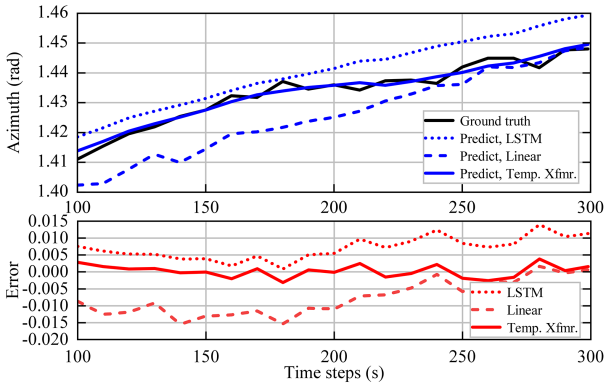


图 6　(网络版彩图) 星间链路方位角的预测.

Figure 6　(Color online) Prediction of the satellite channel azimuth angle.

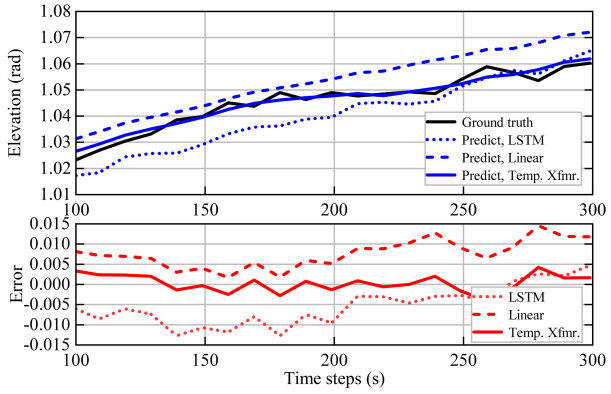


图 7　(网络版彩图) 星间链路俯仰角的预测.

Figure 7　(Color online) Prediction of the satellite channel elevation angle.

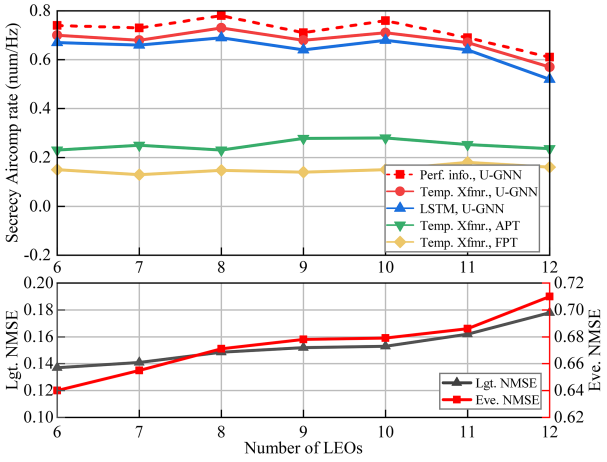


图 8　(网络版彩图) 安全 AirComp 性能随 LEO 卫星数的变化.

Figure 8　(Color online) Secrecy AirComp rate vs. number of LEOs.

优劣; 非学习基线, 包括基于信道反转的自适应功率传输 (APT) 和全功率传输 (FPT), 均基于所提出的时序 Transformer 预测结果进行 AirComp 策略决策. 结果如图 8~11 所示, 仿真指标为系统的平均私密 AirComp 速率 (上方子图), 同时所提方案下的合法端 NMSE 和窃听端 NMSE 变化来揭示性能差异的内在机理 (下方子图).

图 8 给出了系统中参与计算的 LEO 卫星节点数量对性能的影响. 总体而言, 基于深度展开 GNN 的方案能够显著提升 AirComp 的性能, 相比传统信道反转自适应方案和全功率传输方案具有显著的性能优势. 在此基础上, 准确的信道预测能够进一步提升 AirComp 的性能. 与前方信道预测的结果体现的一致, 所提时序预测 Transformer+ 深度展开 GNN 的方案能够很好逼近完美信息条件下的安全 AirComp 性能. 另一方面, 对所有方案而言, 随着发射端 LEO 数量的增多, 所有方案下的 AirComp 性能都有一定的下降. 这是因为更多的聚合信息源意味着需要同时对齐更多的独立信道, 且增加的节点也引入了更多的向窃听者泄露的独立路径, 形成对安全 AirComp 更大的挑战. 从下方子图中可以看到, 随着 LEO 数量的增多, 两个接收端的聚合 NMSE 都有所上升, 聚合难度更大. 但是在所提方案下, 多节点情况下发射波束能够更好地关于合法端对齐聚合, 相应的窃听端的 NMSE 增大更为显著, 表明了所提方案在应对大规模星群协作安全计算时的稳健性.

图 9 评估了 LEO 发射天线数量对系统性能的影响. 随着天线数从 4 增加到 16, 所有方案的安全速率均呈

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

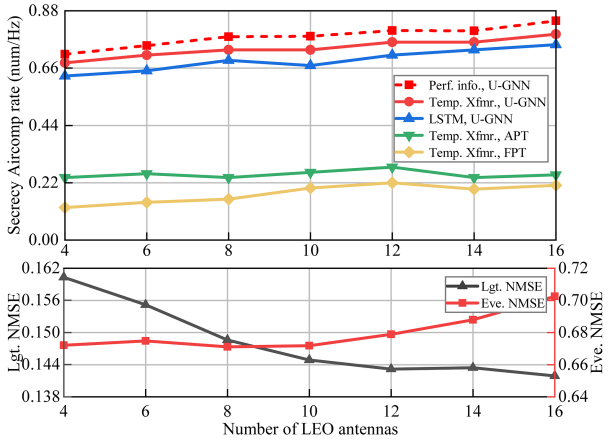


图 9　(网络版彩图) 安全 AirComp 性能随 LEO 卫星天线数的变化.

Figure 9　(Color online) Secrecy AirComp rate vs. number of LEO antennas.

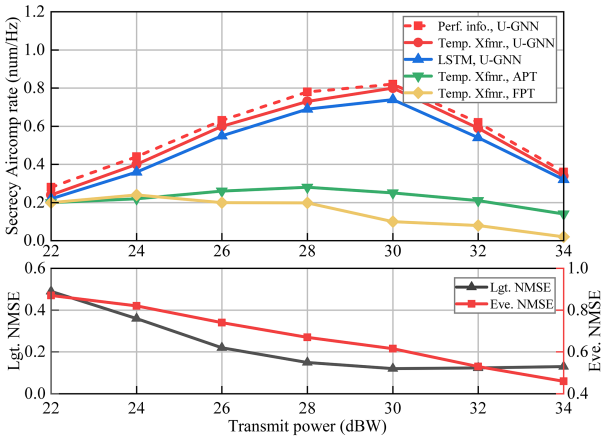


图 10　(网络版彩图) 安全 AirComp 性能随最大发射功率的变化.

Figure 10　(Color online) Secrecy AirComp rate vs. highest transmit power.

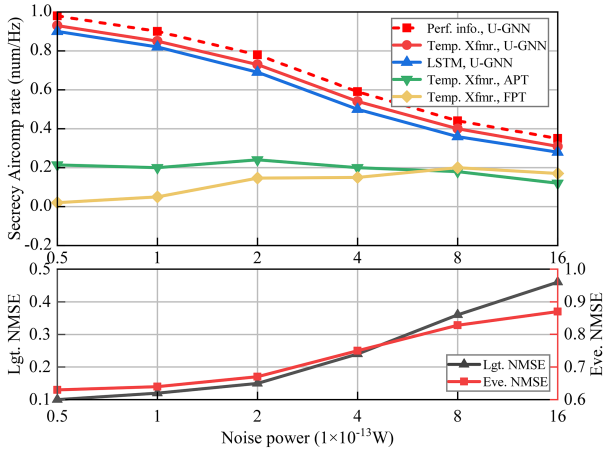


图 11　(网络版彩图) 安全 AirComp 性能随噪声功率的变化.

Figure 11　(Color online) Secrecy AirComp rate vs. noise power.

现稳步上升趋势. 这一现象的物理本质在于多天线带来的空间分集增益, 更多的天线意味着更强的波束成形与干扰抑制能力. 系统可以利用额外的空间自由度产生更窄的主瓣以精准对齐合法 MEO 接收端, 同时在窃听方向形成更深和更宽的空间零陷. 这可以从下方子图中得到佐证, 即在所提方案下, 随着天线数的增加, 合法聚合端的 NMSE 保持下降, 而窃听端的 NMSE 逐渐上升. 此外, 对比不同的方案, 可以类似地观察到, 所提方案始终紧贴完美信息上界, 且与传统启发式 AirComp 策略 (APT/FPT) 的差距随着天线数量的增加而拉大. 这说明传统的启发式算法难以有效利用高维空域资源来兼顾复杂的物理层安全约束, 而基于深度展开的 GNN 能够从数据中学习到更优的波束流形, 充分挖掘了大规模阵列的硬件潜力.

图 10 展示了安全 AirComp 性能随 LEO 最大发射功率变化的趋势. 总体来看, 基于深度展开 GNN 的方案都呈现出明显的先升后降的特征, 其体现了系统从噪声受限向干扰受限的转变过程. 在低功率区间, 系统受热噪声主导, 增加发射功率能显著降低合法端的计算误差, 从而快速提升安全速率. 然而, 当功率进入高功率区间后, 受限于预测误差和天线自由度, 波束成形无法实现完美的干扰对齐或抑制, 泄露到窃听信道的信号能量随发射功率急剧增加, 导致窃听端 NMSE 同样快速下降. 此时, 窃听链路的质量改善速度超过了合法链路, 导致两者的性能间隙收窄, 安全性能反而恶化. 这一现象从下方子图中可以明显看到, 合法端 NMSE 逐渐饱和趋稳, 而窃听

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

端 NMSE 始终能保持下降趋势. 此外, 相比于传统的启发式 AirComp 方案, 所提的深度展开 GNN 能够更智能地在合法对齐与窃听干扰之间寻找平衡点, 保持更好的安全性能.

图 11 显示了背景噪声功率对安全 AirComp 的影响. 显而易见, 随着噪声功率持续增大, 所有方案的性能均呈线性下降. 从下方的 NMSE 子图可以观察到, 噪声增加虽然恶化了窃听者的接收质量, 导致窃听端 NMSE 上升, 但同时也严重破坏了合法信号在空中的模拟叠加精度, 以至于合法链路的性能损失最终主导了整体走向, 导致总私密 AirComp 速率下降. 但是, 在此相对恶劣的条件下, 所提方案依然保持了相对于长短期记忆信道预测和启发式 AirComp 策略的优势, 证明了所提时序 Transformer 对噪声的鲁棒性以及深度展开 GNN 策略在低信噪比环境下维持链路稳定性的能力.

8　结论

本文针对高动态 LEO 卫星网络中高效安全信息聚合需求, 提出了一种物理驱动的 “预测 – 决策” 安全 AirComp 框架. 通过将星间信道解耦为可预测的物理慢变量参数, 实现基于时序 Transformer 的星间信道预测, 并在此基础上基于深度展开 GNN 设计了抗窃听的安全 AirComp 策略. 结果表明, 所提方案能够高精度预测信道演化轨迹, 且能高效生成兼顾聚合精度与物理层抗窃听的波束成形策略. 在不同网络规模、天线配置、发射功率及噪声干扰的环境下, 所提框架均能实现逼近完美信道状态上界的安全 AirComp 速率, 显著优于传统基线方案, 为未来大规模星群网络的高效安全信息协作提供了有力的技术支撑.

参考文献

1 Heo J, Sung S, Lee H, et al. MIMO satellite communication systems: a survey from the PHY layer perspective. IEEE Commun Surv Tut, 2023, 25: 1543–1570
2 Xiao Y, Ye Z, Wu M, et al. Space-air-ground integrated wireless networks for 6G: basics, key technologies, and future trends. IEEE J Sel Areas Commun, 2024, 42: 3327–3354
3 Ntontin K, Lagunas E, Querol J, et al. A vision, survey, and roadmap toward space communications in the 6G and beyond era. Proc IEEE, 2025, 113: 987–1023
4 Yue P, An J, Zhang J, et al. Low earth orbit satellite security and reliability: issues, solutions, and the road ahead. IEEE Commun Surv Tut, 2023, 25: 1604–1652
5 Shi Y M, Zhu J Y, Jiang C X, et al. Satellite edge artificial intelligence with large models: architectures and technologies. Sci China Inf Sci, 2025, 68: 170302
6 Pérez-Neira A, Martinez-Gost M, Şahin A, et al. Waveforms for computing over the air: a groundbreaking approach that redefines data aggregation. IEEE Signal Process Mag, 2025, 42: 57–77
7 Tang X, Xiao H, Shen C, et al. Unfolded deep graph learning for networked over-the-air computation. IEEE Trans Wireless Commun, 2025, 24: 9296–9310
8 Zhu G X, Lyu Z H, Jiao X, et al. Pushing AI to wireless network edge: an overview on integrated sensing, communication, and computation towards 6G. Sci China Inf Sci, 2023, 66: 130301
9 Feng H, Wang R, Liu E, et al. Over-the-air federated learning with joint privacy-accuracy optimization. IEEE Trans Inform Forensic Secur, 2025, 20: 11326–11341
10 Yao J, Wu T, Li Q, et al. Secure beamforming optimization for IRS-assisted MIMO over-the-air computation networks. IEEE Trans Commun, 2025, 73: 8904–8918
11 Hu C, Li Q, Zhang Q, et al. Secure beamforming for integrated sensing, NOMA communication, and over-the-air computation networks. IEEE Trans Inform Forensic Secur, 2025, 20: 10315–10331
12 Khoshafa M H, Bueno F, Ngatched T M N, et al. RIS-empowered secured space-air-ground integrated networks: opportunities and challenges. IEEE Commun Mag, 2025, 63: 130–136
13 Yu J, Liu X, Gao Y, et al. 3D on and off-grid dynamic channel tracking for multiple UAVs and satellite communications. IEEE Trans Wireless Commun, 2022, 21: 3587–3604
14 Lin Z, Gong Y, Huang K. Distributed over-the-air computing for fast distributed optimization: beamforming design and convergence analysis. IEEE J Sel Areas Commun, 2023, 41: 274–287
15 Homssi B A, Chan C C, Wang K, et al. Deep learning forecasting and statistical modeling for Q/V-band LEO satellite channels. Trans Mach Learn Comm Netw, 2023, 1: 78–89

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

16 Zou Y, Wang Z, Chen X, et al. Knowledge-guided learning for transceiver design in over-the-air federated learning. IEEE Trans Wireless Commun, 2023, 22: 270–285
17 Zhu G, Huang K. MIMO over-the-air computation for high-mobility multimodal sensing. IEEE Int Things J, 2019, 6: 6089–6103
18 Zhang R Q, Deng N, Wei H C, et al. D2D-assisted two-stage model aggregation scheme based on over-the-air computation. Sci Sin Inform, 2024, 54: 2487–2502 [张冉强, 邓娜, 卫海超, 等. D2D 辅助的双阶段空中计算模型聚合方案. Sci Sin Inform, 2024, 54: 2487–2502]
19 Liu J, Gong Y, Huang K. Digital over-the-air computation: achieving high reliability via bit-slicing. IEEE Trans Wireless Commun, 2025, 24: 4101–4114
20 Shi W, Yao J C, Xu J D, et al. Empowering over-the-air personalized federated learning via RIS. Sci China Inf Sci, 2024, 67: 219302
21 Lan X, Tang X, Zhang R, et al. UAV-assisted integrated communication and over-the-air computation with interference awareness. IEEE Trans Commun, 2025, 73: 10647–10661
22 Iqbal U, Cho S, Jung H, et al. Performance analysis of physical layer security for over-the-air computation using distributed null-steering beamforming. IEEE Commun Lett, 2025, 29: 303–307
23 Bal M, Marey A, Ates H F, et al. Regression of large-scale path loss parameters using deep neural networks. Antennas Wirel Propag Lett, 2022, 21: 1562–1566
24 Yue T, Liu A, Liang X. Block-based Kalman channel tracking for LEO satellite communication with massive MIMO. IEEE Commun Lett, 2023, 27: 645–649
25 Ying M, Chen X, Qi Q, et al. Deep learning-based joint channel prediction and multibeam precoding for LEO satellite Internet of Things. IEEE Trans Wireless Commun, 2024, 23: 13946–13960
26 Zhang S, Zhang S, Yuan W, et al. Transformer-empowered predictive beamforming for rate-splitting multiple access in non-terrestrial networks. IEEE Trans Wireless Commun, 2024, 23: 19776–19788
27 Hu Z, Liu A, Xu W, et al. A stochastic particle variational bayesian inference inspired deep-unfolding network for sensing over wireless networks. IEEE J Sel Areas Commun, 2024, 42: 2832–2846
28 Hu Q, Shi S, Cai Y, et al. DDPG-driven deep-unfolding with adaptive depth for channel estimation with sparse bayesian learning. IEEE Trans Signal Process, 2022, 70: 4665–4680
29 Nguyen N T, Ma M, Lavi O, et al. Deep unfolding hybrid beamforming designs for THz massive MIMO systems. IEEE Trans Signal Process, 2023, 71: 3788–3804
30 Li B, Verma G, Segarra S. Graph-based algorithm unfolding for energy-aware power allocation in wireless networks. IEEE Trans Wireless Commun, 2023, 22: 1359–1373
31 Schynol L, Pesavento M. Coordinated sum-rate maximization in multicell MU-MIMO with deep unrolling. IEEE J Sel Areas Commun, 2023, 41: 1120–1134

https://www.sciengine.com/doi/10.1360/SSI-2025-0497

Secure inter-satellite AirComp with temporal channel prediction and unfolded graph neural network

Xiao TANG[1,2], Tong HUI[3], Qinghe DU[1], Jinxin LIU[4], Ruonan ZHANG[3] & Chao SHEN[1*]

1. *Faculty of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China*
2. *Shenzhen Research Institute of Northwestern Polytechnical University, Shenzhen 518057, China*
3. *School of Electronics and Information, Northwestern Polytechinical University, Xi'an 710072, China*
4. *School of Mechanical Engineering, Xi'an Jiaotong University, Xi'an 710049, China*

* Corresponding author. E-mail: chaoshen@mail.xjtu.edu.cn

Abstract Low Earth orbit (LEO) satellites, as the critical infrastructure for 6G space-air-ground integrated Networks, face the dual challenges of efficient massive data aggregation and security provisioning. Over-the-air computation (AirComp) leverages wireless waveform superposition to achieve the integration of computation and transmission. While it significantly enhances communication and computation efficiency, its inherent wireless broadcast nature makes it highly vulnerable to eavesdropping attacks. To address these issues, this paper proposes a deep learning-based secure AirComp framework that incorporates channel prediction and secure computation decision-making, targeting highly dynamic inter-satellite links under eavesdropping threats. First, based on prior knowledge of satellite orbital dynamics, a physics-driven channel evolution model is established. A temporal Transformer-based channel prediction network is designed, employing a residual learning paradigm to capture the nonlinear evolution of channel physical parameters from historical observations, thereby achieving high-precision channel prediction. On this basis, a deep unfolding graph neural network (GNN)-based AirComp policy solver is proposed. This solver maps iterative optimization procedures into multi-layer unfolded neural networks and models the interaction and collaboration among different satellite transmitters via message-passing mechanisms, efficiently generating eavesdropping-resilient secure AirComp beamforming strategies. Simulation results demonstrate that the proposed scheme significantly reduces prediction errors, compared to traditional methods. Furthermore, the proposed method achieves near-optimal secure AirComp rate under various network configurations, significantly outperforming existing heuristic baseline schemes.

Keywords LEO satellite, over-the-air computation, channel prediction, graph neural network, Transformer

https://www.sciengine.com/doi/10.1360/SSI-2025-0497