面向车联网V2X网络中GPS欺骗与干扰联合检测的通感一体化

Ali Krayani、Gabriele Barabino、Lucio Marcenaro、Carlo Regazzoni
DITEN，意大利热那亚大学，意大利国家电信跨大学联合体（CNIT）电子邮箱地址：
{ali.krayani}@edu.unige.it，　{lucio.marcenaro、carlo.regazzoni}@unige.it

arXiv:2302.00576v1 [eess.SP] 1 Feb 2023

摘要—**车联网（V2X）通信有望成为第六代（6G）的重要组成部分，以实现智能交通系统（ITS）。仅依赖车载传感器的自动驾驶车辆无法克服安全性和可靠性方面的局限。因此，通感一体化被提出作为一种有效方式，可提升态势感知和自我感知水平，使V2X能够感知物理世界并针对紧急情况调整行为。通过全球定位系统（GPS）实现安全导航对ITS的安全运行至关重要。然而，由于民用GPS接收机缺乏加密和认证机制，欺骗器可以通过发动GPS欺骗攻击轻易复制卫星信号，从而欺骗车辆并篡改导航数据。此外，由于V2X链路具有共享特性，容易遭受可能危及车辆安全的干扰攻击。本文提出一种在V2X网络中联合检测GPS欺骗攻击和干扰攻击的方法。仿真结果表明，所提方法能够以较高的检测概率检测出欺骗器和干扰器。**

索引词—**通感一体化、V2X、6G、GPS欺骗、干扰。**

I. 引言

近年来，车辆技术受到汽车和电信行业的广泛关注，由此推动了车联网通信的发展，以提升道路安全、交通管理服务和驾驶舒适性。第六代（6G）支持的车联网通信被视为实现未来联网自动驾驶车辆的关键推动力 [1]。尽管车联网通信在推动智能交通系统方面具有变革性优势，但仍面临若干技术问题，主要与性能和安全性有关。

感知与通信一体化（ISAC）最近崭露头角，成为6G的一项革命性技术，有望助力未来V2X应用实现自适应学习和智能决策。感知与通信的结合使车辆能够更好地感知周围环境，预测附近用户的机动动作并做出智能决策，从而为构建更安全的交通系统铺平道路 [2]。现代化车辆配备了多种传感器，可分为用于观测周围环境的外感受传感器和用于观测自身状态的本体感受传感器。前者包括GPS、激光雷达和摄像头，有助于提升态势感知；而后者包括转向、踏板和车轮速度等传感器，有助于提升自我感知。

车辆在感知环境的同时，可以交换消息，以增强态势感知和自我感知，并协调与其他车辆的行驶操作。这些消息，如基本安全消息（BSM）和协同感知消息（CAM），包含发送车辆的状态信息（如位置和速度），以及附近其他车辆的状态信息。车辆可以使用摄像头和激光雷达等传感器检测道路使用者（例如行人），并通过车联网消息将相关信息传达给其他道路使用者，从而提升整体性能。然而，由于车辆与其他蜂窝用户共享无线频谱且无线频谱具有开放性，承载这些消息的车联网通信链路容易受到恶意攻击 [3]。例如，附近的干扰器可能会篡改要传达给附近车辆/用户的信息，也可能蓄意中断车辆编队之间的通信，使车载单元（OBU）和/或路侧单元（RSU）无法识别合法信号，从而危及车辆安全 [4]。

此外，GPS信号的完整性以及正确获取用于计算位置、速度和时间信息的导航数据，对V2X应用的安全运行至关重要。然而，由于民用GPS接收机依赖未加密的卫星信号，欺骗器可以轻易伪造这些信号，诱骗GPS接收机计算出虚假的位置 [5]。此外，卫星与地面GPS接收机之间的距离很远，导致信号极其微弱，很容易被欺骗器发出的信号淹没。因此，GPS传感器易受欺骗攻击，这构成了严重威胁，可能导致车辆失控甚至遭劫持，危及人类生命 [6]。因此，必须实时管控并检测GPS欺骗攻击和干扰，以实现安全的车载通信，使车辆能够安全地相互通信并与基础设施（例如路侧终端、基站）交互 [7]。

现有的 GPS 欺骗检测方法包括 GPS 信号分析方法和 GPS 消息加密方法[8]。然而，前者在检测过程中需要真实数据源，而这并非总是能够获取。相比之下，后者需要 GPS 接收机配备安全基础设施和先进的计算资源，这

阻碍了其在 V2X 应用中的推广。另一方面，现有的车载网络干扰器检测方法基于分析丢包率，如 [9]，所示，因此难以检测通过操纵合法信号而非干扰信号来进行攻击的高级干扰器。在本研究中，我们提出一种在 V2X 网络中联合检测 GPS 欺骗和干扰攻击的方法。我们采用耦合广义动态贝叶斯网络（C-GDBN），学习路侧单元从多辆车接收的射频信号与相应轨迹之间的交互。将车辆位置信息与车载基础设施（V2I）通信相结合，既可在将射频信号与车辆轨迹关联时进行语义学习，也使路侧单元能够联合预测其预期从车辆接收的射频信号，并据此预测预期轨迹。

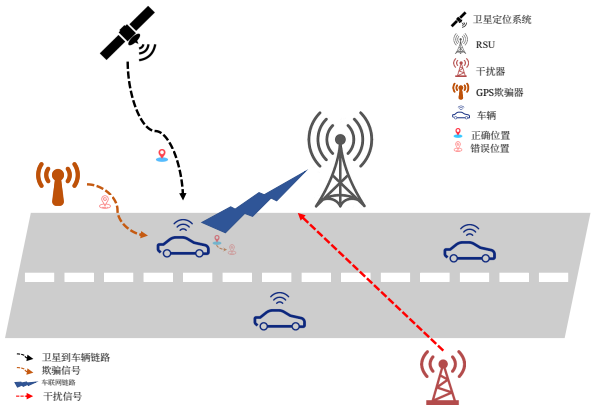

图 1. 系统模型示意图。

本文的主要贡献可概括如下：*i)* 针对 V2X 场景，提出一种联合 GPS欺骗与干扰检测方法，该方法基于学习生成式交互模型 C-GDBN。该模型对多辆车辆发射的射频信号与其轨迹之间的互相关进行编码，并在较高抽象层次上随机耦合二者的语义含义。*ii)* 配备所获得的 C-GDBN 的认知路侧单元能够根据实时射频信号预测并估计车辆位置。这使路侧单元能够评估射频信号和车辆轨迹是否均按照 C-GDBN 中编码的动态规则演变，进而识别 V2X环境中出现异常行为的原因（即干扰器攻击 V2I，或欺骗器攻击卫星链路）。*iii)* 大量仿真结果表明，所提方法能够根据预测的射频信号准确估计车辆轨迹，有效检测异常行为，并以较高的检测概率识别异常类型。据我们所知，这是首项研究 V2X系统中干扰与欺骗联合检测的工作。

II. 系统模型与问题表述

图 1 所示的系统模型包含一个由路侧单元（RSU）组成的单小区车联网

位于 $\mathbf{p}_R = [x_R, y_R]$ 的路侧干扰器 (RSJ)、位于 $\mathbf{p}_J = [x_J, y_J]$ 的路侧欺骗器 (RSS)，以及在城市区域多车道道路上行驶的 N 辆车辆。第 n 辆车辆随时间变化的位置表示为 $\mathbf{p}_{n,t} = [x_{n,t}, y_{n,t}]$ 其中 $n \in N$。在可用于车联网 (V2I) 通信的 K 个正交子信道中，RSU 为每辆车分配一条 V2I 链路。每辆车在每个时刻 t 通过第 k 条 V2I 链路向 RSU 发送承载这些消息的信号 $\mathbf{x}_{t,k}$，以交换由车辆状态（即位置和速度）组成的消息，其中 $k \in K$。我们考虑一个反应式路侧干扰器，它旨在通过向通信链路注入故意干扰来攻击 V2I 链路从而改变车辆发送的信号。这与此相反，路侧欺骗器旨在通过欺骗 GPS 信号误导车辆，使其登记错误的 GPS位置。RSU 旨在检测卫星链路上的欺骗器以及多条 V2I 链路上的干扰器，以采取有效措施并保护车载网络。联合 GPS欺骗与干扰检测问题可表述为以下三元假设检验：

$$\begin{cases} \mathcal{H}_0 : \mathrm{z}_{t,k} = \mathrm{g}_{t,k}^{nR}\mathrm{x}_{t,k} + \mathrm{v}_{t,k}, \\ \mathcal{H}_1 : \mathrm{z}_{t,k} = \mathrm{g}_{t,k}^{nR}\mathrm{x}_{t,k} + \mathrm{g}_{t,k}^{JR}\mathrm{x}_{t,k}^{j} + \mathrm{v}_{t,k}, \\ \mathcal{H}_2 : \mathrm{z}_{t,k} = \mathrm{g}_{t,k}^{nR}\mathrm{x}_{t,k}^{*} + \mathrm{v}_{t,k}, \end{cases} \tag{1}$$

其中，$\mathcal{H}_0$、$\mathcal{H}_1$ 和 $\mathcal{H}_2$ 分别表示三种假设，对应于干扰器和欺骗器均不存在、干扰器存在以及欺骗器存在。$\mathrm{z}_{t,k}$ 表示RSU在 t 处通过第 k条V2I链路接收到的信号，$\mathrm{g}_{t,k}^{nR}$ 表示从车辆 n 到RSU的信道功率增益，其公式为：$\mathrm{g}_{t,k}^{nR} = \alpha_{t,k}^{nR}\mathrm{h}_{t,k}^{nR}$，其中$\alpha_{t,k}^{nR}$表示包含路径损耗和阴影衰落的大尺度衰落，建模为 [10]: $\alpha_{t,k}^{nR} = G\beta d_{t,nR}^{-\gamma}$。$G$ 为路径损耗常数，β为对数正态阴影衰落随机变量，$d_{t,nR} = \sqrt{(x_{n,t} - x_R)^2 + (y_{n,t} - y_R)^2}$ 表示第 n辆车辆与RSU之间的距离。γ 为功率衰减指数，$\mathrm{h}_{t,k}$ 为小尺度衰落分量，其服从 $\mathcal{CN}(0, 1)$分布。此外，$\mathrm{x}_{t,k}$ 为第 n辆车辆发送的目标信号，$\mathrm{v}_{t,k}$ 为方差为 σ_n^2的加性高斯白噪声。$\mathrm{x}_{t,k}^{J}$ 为干扰信号，$\mathrm{x}_{t,k}^{*}$ 为欺骗信号（即承载与错误GPS位置相关比特的信号），$\mathrm{g}_{t,k}^{JR} = \alpha_{t,k}^{JR}\mathrm{h}_{t,k}^{JR}$，$\mathrm{h}_{t,k}^{JR}$ 为从RSJ到RSU的信道功率增益，其中$\alpha_{t,JR}^{JR} = G\beta d_{t,JR}^{-\gamma}$，$JR$ 满足$d_{t,JR} = \sqrt{(x_J - x_R)^2 + (y_J - y_R)^2}$。我们假设V2I链路的信道状态信息（CSI）已知，并且RSU可以按照 [11]中的方法对其进行估计。RSU配备有射频天线，在对接收到的射频信号进行解码后，可以跟踪车辆的轨迹。RSU旨在学习从多辆车辆接收到的射频信号与其对应轨迹之间的交互关系。

A. 环境表示

RSU接收来自每辆车辆的射频信号，并通过对接收到的射频信号进行解码和解调来跟踪其轨迹（我们将其称为GPS信号）。描述第 i个信号在多个层级上演化的广义状态空间模型包含以下方程：

$$\tilde{\mathrm{S}}_{\mathrm{t}}^{(i)} = \mathrm{f}(\tilde{\mathrm{S}}_{\mathrm{t-1}}^{(i)}) + \tilde{\mathrm{w}}_t, \tag{2}$$

$$\tilde{\mathrm{X}}_{\mathrm{t}}^{(i)} = \mathrm{A}\tilde{\mathrm{X}}_{\mathrm{t-1}}^{(i)} + \mathrm{BU}_{\tilde{\mathrm{S}}_{\mathrm{t}}^{(i)}} + \tilde{\mathrm{w}}_t, \tag{3}$$

$$\tilde{\mathrm{Z}}_{\mathrm{t}}^{(i)} = \mathrm{H}\tilde{\mathrm{X}}_{\mathrm{t}}^{(i)} + \tilde{\mathrm{v}}_t, \tag{4}$$

其中， $i \in \{\mathrm{RF}, \mathrm{GPS}\}$ 表示路侧单元接收到的信号类型。(2) 中定义的转移系统模型解释了离散随机变量 $\tilde{\mathrm{S}}^{(i)}{}_{\mathrm{t}}$ 的演变，这些变量表示射频信号（或 GPS 信号）动态中的簇；f(.) 是关于其自变量的非线性函数，加性项$\tilde{\mathrm{w}}_t$ 表示过程噪声。(3) 中定义的动态模型解释了射频信号动态的演变，或第 n 辆车辆的运动动态演变，其中 $\tilde{\mathrm{X}}^{(i)}{}_{\mathrm{t}}$ 是生成传感信号的隐连续变量，$\mathrm{A} \in \mathbb{R}^{2d}$ 和 $\mathrm{B} \in \mathbb{R}^{2d}$ 分别是动态矩阵和控制矩阵，而 $\mathrm{U}^{\tilde{\mathrm{S}}^{(i)}}{}_{\mathrm{t}}$ 是控制向量，表示信号随时间演变的动态规则。(4) 中定义的测量模型描述了传感信号 $\tilde{\mathrm{Z}}^{(i)}{}_{\mathrm{t}}$ 与隐状态 $\tilde{\mathrm{X}}^{(i)}{}_{\mathrm{t}}$ 之间的依赖关系，该关系由测量矩阵 $\mathrm{B} \in \mathbb{R}^{2d}$ 参数化，其中 d 表示数据维度， $\tilde{\mathrm{v}}_t$ 表示随机噪声。

B. 学习 *GDBN*

式 (2)、(3) 和 (4) 中定义的层级动态模型采用广义动态贝叶斯网络（GDBN） [12] 进行结构化，如图 2-(a) 所示。该概率图模型表达了随机隐变量与可观测状态之间的条件依赖关系。用于解释传感信号如何生成的生成过程可分解为：

$$\mathrm{P}(\tilde{\mathrm{Z}}_t^{(i)}, \tilde{\mathrm{X}}_t^{(i)}, \tilde{\mathrm{S}}_t^{(i)}) = \mathrm{P}(\tilde{\mathrm{S}}_0^{(i)})\mathrm{P}(\tilde{\mathrm{X}}_0^{(i)}) \left[\prod_{t=1}^{\mathrm{T}} \mathrm{P}(\tilde{\mathrm{Z}}_t^{(i)}|\tilde{\mathrm{X}}_t^{(i)})\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{X}}_{t-1}^{(i)}, \tilde{\mathrm{S}}_t^{(i)})\mathrm{P}(\tilde{\mathrm{S}}_t^{(i)}|\tilde{\mathrm{S}}_{t-1}^{(i)})\right], \tag{5}$$

其中，$\mathrm{P}(\tilde{\mathrm{S}}_0^{(i)})$ 和 $\mathrm{P}(\tilde{\mathrm{X}}_0^{(i)})$ 是初始先验分布，$\mathrm{P}(\tilde{\mathrm{Z}}_t^{(i)}|\tilde{\mathrm{X}}_t^{(i)})$ 是似然，$\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{X}}_{t-1}^{(i)}, \tilde{\mathrm{S}}_t^{(i)})$ 和 $\mathrm{P}(\tilde{\mathrm{S}}_t^{(i)}|\tilde{\mathrm{S}}_{t-1}^{(i)})$ 是转移密度，用于描述广义状态空间模型的时间动态和层级动态。式 (5) 中定义的生成过程表明了模型施加于随机变量 $\tilde{\mathrm{S}}_t^{(i)}$、$\tilde{\mathrm{X}}_t^{(i)}$ 和 $\tilde{\mathrm{Z}}_t^{(i)}$ 上的因果关系，从而形成一条因果链——描述一种状态如何促成另一种状态的生成，这由链接 $\tilde{\mathrm{S}}_t^{(i)} \rightarrow \tilde{\mathrm{X}}_t^{(i)} \rightarrow \tilde{\mathrm{Z}}_t^{(i)}$ 表示。

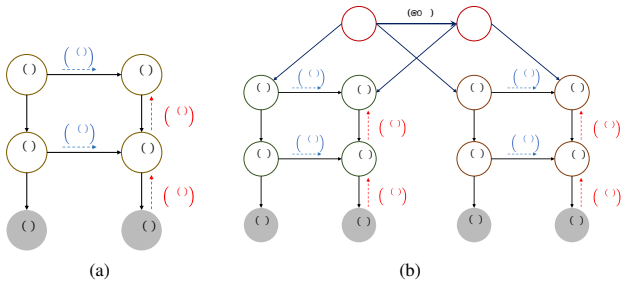

图 2。（a）GDBN。（b）耦合 GDBN（C-GDBN），由两个 GDBN 组成，分别表示路侧单元接收的两个信号，其离散隐变量以随机方式耦合。

路侧单元开始感知环境时，对环境状态的演化采用静态假设，即假定传感信号仅受随机噪声影响。因此，路侧单元使用以下简化模型预测射频信号（或车辆轨迹）：$\tilde{\mathrm{X}}_t^{(i)} = \mathrm{A}\tilde{\mathrm{X}}_{t-1}^{(i)} + \tilde{\mathrm{w}}_t$。该模型与式（3）的区别在于控制向量 $\mathrm{U}^{\tilde{\mathrm{S}}^{(i)}}{}_{\mathrm{t}}$ 被假定为零，即 $\mathrm{U}^{\tilde{\mathrm{S}}^{(i)}}{}_{\mathrm{t}} = 0$ ，因为尚未发现用于解释环境状态如何随时间演化的动态规则。通过利用广义误差（GE），即可发现这些规则；广义误差是预测与观测之间的差值。投影到测量空间中的广义误差计算如下：$\tilde{\varepsilon}_{\tilde{\mathrm{Z}}_t^{(i)}} = \tilde{\mathrm{Z}}_t^{(i)} - \mathrm{H}\tilde{\mathrm{X}}_t^{(i)}$。将 $\tilde{\varepsilon}_{\tilde{\mathrm{Z}}_t}$ 投影回广义状态空间可按如下方式进行：

$$\tilde{\varepsilon}_{\tilde{\mathrm{X}}_t}^{(i)} = \mathrm{H}^{-1}\tilde{\varepsilon}_{\tilde{\mathrm{Z}}_t^{(i)}} = \mathrm{H}^{-1}(\tilde{\mathrm{Z}}_t^{(i)} - \mathrm{H}\tilde{\mathrm{X}}_t^{(i)}) = \mathrm{H}^{-1}\tilde{\mathrm{Z}}_t^{(i)} - \tilde{\mathrm{X}}_t^{(i)}. \tag{6}$$

式（6）中定义的 GE 可通过增长神经气（GNG）以无监督方式划分为离散簇。后者生成一组离散变量（簇），表示为：$\tilde{\mathbf{S}}^{(\mathbf{i})} = \{\tilde{\mathrm{S}}_1^{(i)}, \tilde{\mathrm{S}}_2^{(i)}, \ldots, \tilde{\mathrm{S}}_{M_i}^{(i)}\}$，其中 M_i 为簇的总数，每个簇 $\tilde{\mathrm{S}}_m^{(i)} \in \tilde{\mathbf{S}}^{(\mathbf{i})}$ 均服从由具有同质属性的 GE 组成的高斯分布，因此 $\tilde{\mathrm{S}}_m^{(i)} \sim \mathcal{N}(\tilde{\mu}_{\tilde{\mathrm{S}}_m^{(i)}} = [\mu_{\tilde{S}_m^{(i)}}, \dot{\mu}_{\tilde{S}_m^{(i)}}]\ \Sigma_{\tilde{\mathrm{S}}_m^{(i)}})$。

通过估计时变转移概率 $\pi_{ij} = \mathrm{P}(\tilde{\mathrm{S}}_t^{(i)} = i|\tilde{\mathrm{S}}_{t-1}^{(i)} = j, \tau)$，可以在时变转移矩阵（$\Pi_\tau$）中捕获传感信号在可用簇之间的动态转移，其中 τ 表示在 $\tilde{\mathrm{S}}_{t-1}^{(i)} = j$ 中经过的时间，之后转移至 $\tilde{\mathrm{S}}_t^{(i)} = i$。

C. 耦合 *GDBN* 的学习 （*C-GDBN*）

上一节所述的学习过程可以针对每种信号类型分别执行，即射频信号和GPS。为每种信号类型分别学习一个GDBN模型后，我们通过跟踪某次经历期间在路侧单元接收到的射频信号与GPS信号之间的簇激活，分析二者的交互行为。此类交互可以编码在如图2-(b)所示的耦合GDBN（C-GDBN）中，该模型由分别表示两种信号的两个GDBN组成，其中它们在离散层级上的隐变量在 $\tilde{\mathrm{C}}_t = [\tilde{\mathrm{S}}_t^{(1)}, \tilde{\mathrm{S}}_t^{(2)}]$ 中以随机方式耦合，因为这些变量彼此不相关，但其均值相互耦合。交互

矩阵 $\Phi \in \mathbb{R}^{M_1,\ M_2}$ 对激发簇模式进行编码，从而能够根据射频信号预测GPS信号，其定义如下：

$$\Phi = \begin{bmatrix} \mathrm{P}(\tilde{\mathrm{S}}_1^{(2)}|\tilde{\mathrm{S}}_1^{(1)}) & \mathrm{P}(\tilde{\mathrm{S}}_2^{(2)}|\tilde{\mathrm{S}}_1^{(1)}) & \dots & \mathrm{P}(\tilde{\mathrm{S}}_{\mathrm{M}_2}^{(2)}|\tilde{\mathrm{S}}_1^{(1)}) \\ \mathrm{P}(\tilde{\mathrm{S}}_1^{(2)}|\tilde{\mathrm{S}}_2^{(1)}) & \mathrm{P}(\tilde{\mathrm{S}}_2^{(2)}|\tilde{\mathrm{S}}_2^{(1)}) & \dots & \mathrm{P}(\tilde{\mathrm{S}}_{\mathrm{M}_2}^{(2)}|\tilde{\mathrm{S}}_2^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{P}(\tilde{\mathrm{S}}_1^{(2)}|\tilde{\mathrm{S}}_{\mathrm{M}_1}^{(1)}) & \mathrm{P}(\tilde{\mathrm{S}}_2^{(2)}|\tilde{\mathrm{S}}_{\mathrm{M}_1}^{(1)}) & \dots & \mathrm{P}(\tilde{\mathrm{S}}_{\mathrm{M}_2}^{(2)}|\tilde{\mathrm{S}}_{\mathrm{M}_1}^{(1)}) \end{bmatrix}. \tag{7}$$

D. 联合预测与感知

路侧单元（RSU）开始使用改进马尔可夫跳跃粒子滤波器（M-MJPF） [12] 预测其预期从每辆车接收到的射频信号。该滤波器结合了粒子滤波器（PF）和卡尔曼滤波器（KF），用于进行时间和层次预测。由于所获得的 C-GDBN 能够根据另一信号的动态演化来预测某一信号的动态演化，因此需要一种能够处理更复杂预测的交互式贝叶斯滤波器。为此，我们提出在 C-GDBN 上使用交互式改进马尔可夫跳跃粒子滤波器（IM-MJPF）。IM-MJPF 包含一个粒子滤波器，用于传播一组权重相等的 L 粒子，使得 $\{\tilde{\mathrm{S}}_{t\,l}^{(1)},,\mathrm{W}_t^{(1)},_l\}\sim\{\pi(\tilde{\mathrm{S}}_t^{(1)})\ \frac{1}{L}\}$，其中 $\tilde{\mathrm{S}}_{t\,l}^{(1)},, l \in L$，且 $(.^{(1)})$为射频信号类型。此外，路侧单元依赖于式（7）中定义的 Φ，从预测的射频信号出发，预测 $\tilde{\mathrm{S}}_t^{(2)}$，以实现车辆轨迹的离散簇，具体如下：$\{\tilde{\mathrm{S}}_t^{(2)},\mathrm{W}_t^{(2)},_l\}\sim\{\Phi(\tilde{\mathrm{S}}_{t\,l}^{(1)},)=\mathrm{P}(.|\tilde{\mathrm{S}}_{t\,l}^{(1)},),\mathrm{W}_t^{(2)},_l\}$。对于每个预测的离散变量 $\tilde{\mathrm{S}}_{t\,l}^{(i)},,$ 均采用多重卡尔曼滤波器来预测多个连续变量；这些预测受较高层级预测的引导，如式（3）所述，可用概率形式表示为 $\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{X}}_{t-1}^{(i)},\tilde{\mathrm{S}}_t^{(i)})$。用于评估期望的后验概率为：

$$\pi(\tilde{\mathrm{X}}_t^{(i)}) = \mathrm{P}(\tilde{\mathrm{X}}_t^{(i)},\tilde{\mathrm{S}}_t^{(i)}|\tilde{\mathrm{Z}}_{t-1}^{(i)}) = \int \mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{X}}_{t-1}^{(i)},\tilde{\mathrm{S}}_t^{(i)})\lambda(\tilde{\mathrm{X}}_{t-1}^{(i)})d\tilde{\mathrm{X}}_{t-1}^{(i)}, \tag{8}$$

其中 $\lambda(\tilde{\mathrm{X}}_{t-1}^{(i)})=\mathrm{P}(\tilde{\mathrm{Z}}_{t-1}^{(i)}|\tilde{\mathrm{X}}_{t-1}^{(i)})$。观察到新证据 $\tilde{\mathrm{Z}}_t^{(i)}$ 后，可通过以下形式利用诊断消息 $\lambda(\tilde{\mathrm{X}}_t^{(i)})$ 更新后验分布（从而表示更新后的信念）：$\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)},\tilde{\mathrm{S}}_t^{(i)}|\tilde{\mathrm{Z}}_t^{(i)})=\pi(\tilde{\mathrm{X}}_t^{(i)})\lambda(\tilde{\mathrm{X}}_t^{(i)})$。同样，离散隐变量的信念也可以按照以下方式更新：$\mathrm{W}_t^{(i)},_l=\mathrm{W}_t^{(i)},_l\lambda(\tilde{\mathrm{S}}_t^{(i)})$，其中：$\lambda(\tilde{\mathrm{S}}_t^{(i)})=\lambda(\tilde{\mathrm{X}}_t^{(i)})\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{S}}_t^{(i)})=\mathrm{P}(\tilde{\mathrm{Z}}_t^{(i)}|\tilde{\mathrm{X}}_t^{(i)})\mathrm{P}(\tilde{\mathrm{X}}_t^{(i)}|\tilde{\mathrm{S}}_t^{(i)})$。

*E. GPS*欺骗与干扰联合检测

路侧单元可以根据 IM-MJPF 生成的多重异常指标评估当前情况，并识别 V2I 是否受到攻击，或卫星链路是否遭到欺骗。第一个指标计算预测射频信号与观测射频信号之间的相似度，其定义如下：

$$\Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} = -ln\Big(\mathcal{BC}\big(\pi(\tilde{\mathrm{X}}_t^{(1)}),\lambda(\tilde{\mathrm{X}}_t^{(1)})\big)\Big), \tag{9}$$

其中 $\mathcal{BC}(.)=\int\sqrt{\pi(\tilde{\mathrm{X}}_t^{(1)})\ \lambda(\tilde{\mathrm{X}}_t^{(1)})}d\tilde{\mathrm{X}}_t^{(1)}$ 为巴氏系数。第二个指标计算对射频信号进行解码后，预测的 GPS信号（由射频信号得到）与观测 GPS信号之间的相似度，其定义如下：

$$\Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} = -ln\Big(\mathcal{BC}\big(\pi(\tilde{\mathrm{X}}_t^{(2)}),\lambda(\tilde{\mathrm{X}}_t^{(2)})\big)\Big), \tag{10}$$

其中 $\mathcal{BC}(。)=\int\sqrt{\pi(\tilde{\mathrm{X}}_t^{(2)})\ \lambda(\tilde{\mathrm{X}}_t^{(2)})}d\tilde{\mathrm{X}}_t^{(2)}$。RSU可识别不同的假设，以了解当前情况，即：是否存在攻击 V2I链路的干扰器，或攻击卫星与车辆之间链路的欺骗器，或者干扰器和欺骗器均不存在，具体如下：

$$\begin{cases} \mathcal{H}_0 : \text{if}\ \ \Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} < \xi_1 \text{ and } \Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} < \xi_2, \\ \mathcal{H}_1 : \text{if}\ \ \Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} \geq \xi_1 \text{ and } \Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} \geq \xi_2, \\ \mathcal{H}_2 : \text{if}\ \ \Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} < \xi_1 \text{ and } \Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} \geq \xi_2, \end{cases} \tag{11}$$

其中 $\xi_1 = \mathbb{E}[\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(1)}}] + 3\sqrt{\mathbb{V}[\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(1)}}]}$，以及 $\xi_2 = \mathbb{E}[\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(2)}}] + 3\sqrt{\mathbb{V}[\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(2)}}]}$。在 ξ_1 和 ξ_2中，$\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(1)}}$ 和 $\bar{\Upsilon}_{\tilde{\mathrm{X}}_t^{(2)}}$ 表示训练期间的异常信号（即不存在干扰器和欺骗器时的正常情况）。

F. 评估指标

为了评估所提出方法联合检测干扰器和 GPS 欺骗器的性能，我们分别采用干扰器检测概率（P_d^j）和欺骗器检测概率（P_d^s），其定义如下：

$$\mathrm{P}_d^j = \Pr(\Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} \geq \xi_1, \Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} \geq \xi_2 | \mathcal{H}_1), \tag{12}$$

$$\mathrm{P}_d^s = \Pr(\Upsilon_{\tilde{\mathrm{X}}_t^{(1)}} < \xi_1, \Upsilon_{\tilde{\mathrm{X}}_t^{(2)}} \geq \xi_2 | \mathcal{H}_2). \tag{13}$$

此外，我们采用如下定义的均方根误差（RMSE），评估所提出方法在预测和估计车辆轨迹及预期射频信号方面的准确性：

$$RMSE = \sqrt{\frac{1}{T}\sum_{t=1}^{T}\left(\tilde{\mathrm{Z}}_t^{(i)} - \tilde{\mathrm{X}}_t^{(i)}\right)^2}, \tag{14}$$

其中，T 为预测总数。

IV. 仿真结果

在本节中，我们通过大量仿真评估所提出方法联合检测干扰器和欺骗器的性能。我们考虑 $\mathrm{N} = 2$ 辆车辆在环境中交互，并与路侧单元交换其状态（即位置和速度）。车辆沿预定义轨迹行驶，执行各种路口行驶操作，这些操作选自 [13]提出的*Lankershim* 数据集。该数据集描述了一个四岔路口，包含约 19 种路口行驶操作。路侧单元为每辆车分配一个子信道，以实现 V2I 链路，车辆状态通过该链路传输。承载车辆状态的发射信号

和干扰信号均采用 QPSK 调制。仿真设置如下：载波频率为 2GHz，带宽为=1.4MHz，小区半径为 500m；路侧单元天线高度和增益分别为 25m 和 8 dBi；接收机噪声系数为 5dB；车辆天线高度和增益分别为 1.5m 和 3dBi；车辆速度为 40Km/h；V2I发射功率为 23dBm；干扰器发射功率范围为 20dBm 至 40dBm；信噪比为 20dB；路径损耗模型为（$128.1+37.6logd$）；对数正态阴影衰落的标准差为 8dB，快衰落信道服从瑞利分布。

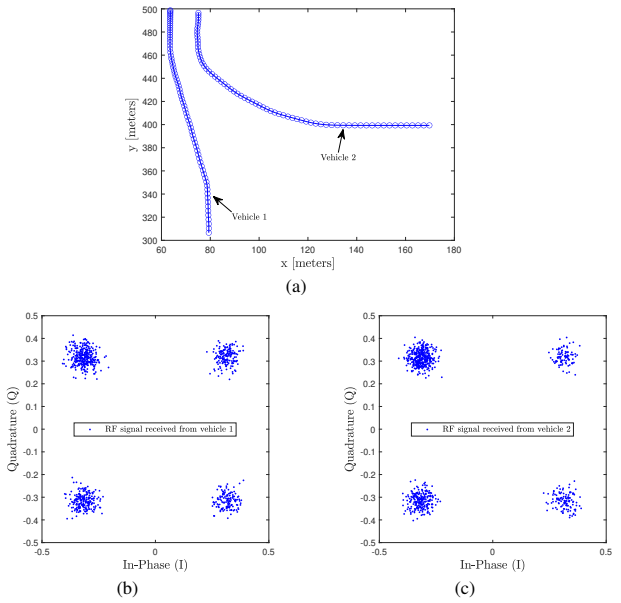

图3. 一个示例，展示了从两辆车辆接收到的射频信号及其对应的轨迹：(a) 车辆的轨迹，(b) 从车辆1接收到的射频信号，(c) 从车辆2接收到的射频信号。

路侧单元旨在学习多个交互模型（即 C-GDBN模型），以编码从每辆车辆接收到的射频信号与其对应轨迹之间的交叉关系。这些模型使路侧单元能够根据接收到的射频信号预测车辆将遵循的轨迹，并评估 V2I 是否遭受干扰攻击，或卫星链路是否受到欺骗。需要注意的是，路侧单元仅接收来自两辆车辆的射频信号，并在解码这些射频信号后获取它们的位置。因此，路侧单元应能够评估接收到的射频信号是否按照迄今为止学到的动态规则变化，以及车辆是否遵循预期的（正确）轨迹，从而判断 V2I 链路是否确实遭受攻击，或卫星链路是否受到欺骗。

图3-(a)展示了两辆车辆执行特定机动动作时交互的示例，图3-(b)展示了路侧单元接收到的来自两辆车辆的射频信号。在学习过程开始时，路侧单元根据（3）中定义的简化模型进行预测，其中 $U^{\tilde{S}^{(i)}}{}_t=0$。在获得（6）中指出的广义误差后，RUS 使用 GNG 对这些误差进行聚类，以学习两个编码动态规则的 GDBN 模型

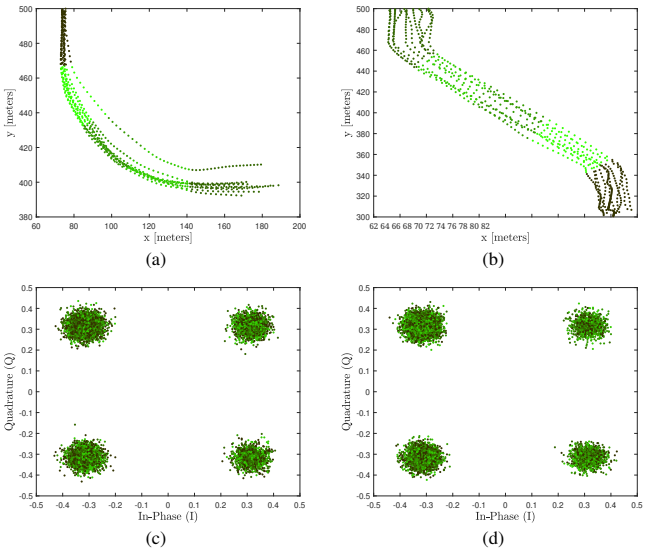

图4. 对不同经历中获得的广义误差进行聚类后 GNG 的输出：(a) 车辆1的聚类轨迹，(b) 车辆2的聚类轨迹，(c) 从车辆1接收到的聚类射频信号，(d) 从车辆2接收到的聚类射频信号。

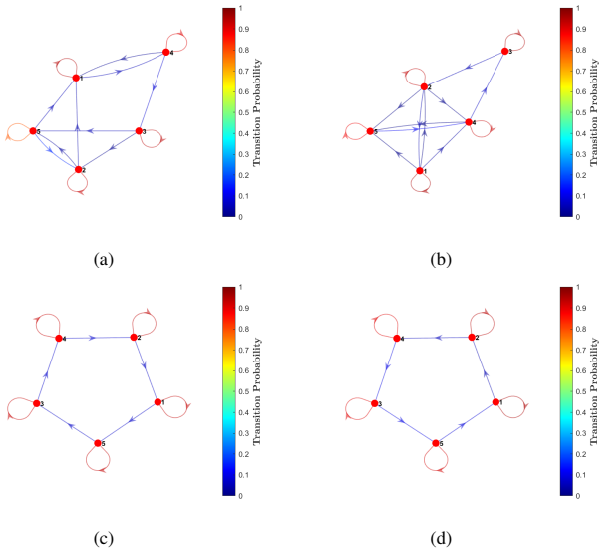

图5. 转移矩阵（TM）的图形表示：(a) 与车辆1轨迹相关的 TM，(b) 与车辆2轨迹相关的 TM，(c) 与从车辆1接收到的射频信号相关的 TM，(d) 与从车辆2接收到的射频信号相关的 TM。

分别描述射频信号和GPS信号随时间的变化情况，如图4和图5所示。路侧单元可以通过学习编码在C-GDBN中的交互转移矩阵，将这两个GDBN耦合起来，如图6所示。

图 7 展示了一个示例，比较了采用两种不同配置学习交互矩阵（如图 6 所示）时预测的射频信号与观测到的射频信号。此外，图 8 展示了一个示例，比较了使用图 6 所示的两个交互矩阵时两辆车辆的预测轨迹与观测轨迹，

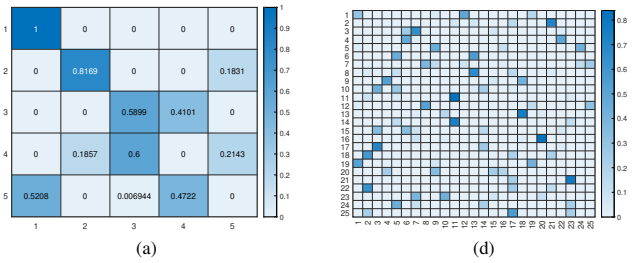

图 6. 使用不同配置定义的式 (7) 中的交互转移矩阵：(a) $M_1 = 5, M_2 = 5$；(b) $M_1 = 25, M_2 = 25$。

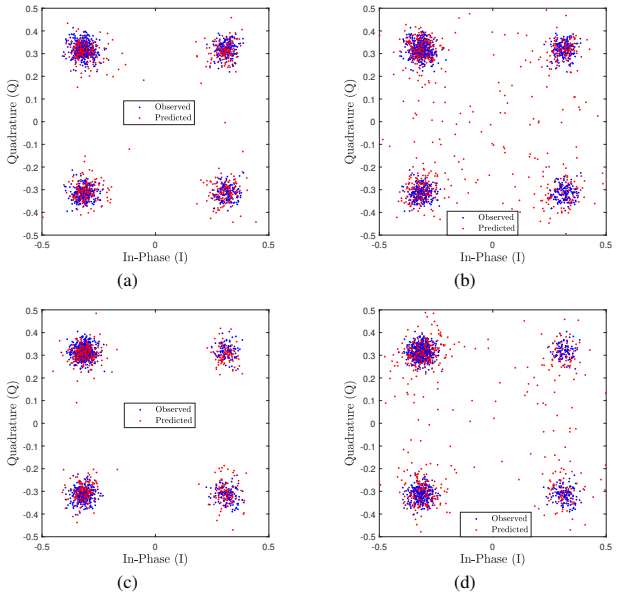

图 7. 不同配置下，2 辆车辆发射的预测和观测射频信号示例。预测射频信号来自：(a) 使用 M_1=5, M_2=5 的车辆1；(b) 使用 M_1=25, M_2=25 的车辆1；(c) 使用 M_1=5, M_2=5 的车辆2；(d) 使用 M_1=25, M_2=25 的车辆2。

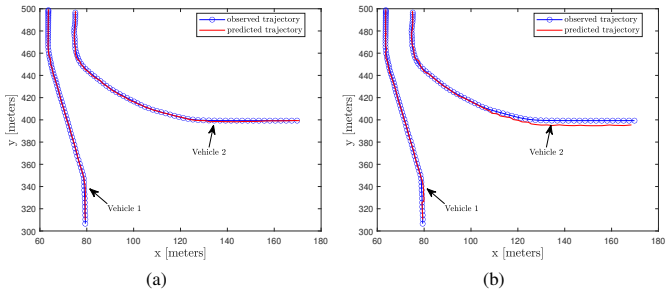

图 8. 两辆车辆在环境中交互时，其预测和观测轨迹的示例。(a) M_1=5, M_2=5；(b) M_1=25, M_2=25。

我们可以从图 7 和图 8 看出，与使用簇数较多的交互矩阵相比，使用簇数较少的交互矩阵能够获得更好的预测效果。这一点可以通过观察图 9 得到验证。

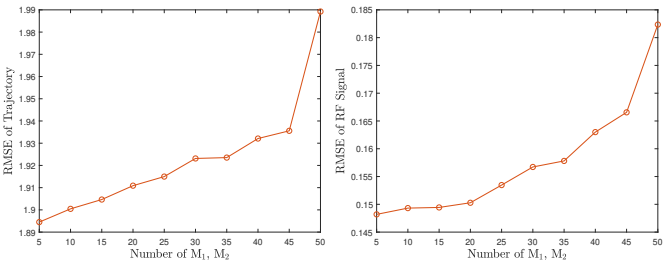

图 9. 测试不同经历后的平均均方根误差，以及以下内容的示例：(a) 轨迹和 (b) 射频信号。

该图展示了两个模型在不同簇数量下的均方根误差值，这两个模型分别描述接收射频信号的动态特性和车辆轨迹。可以看出，随着簇数量增加，均方根误差也会增大，因为增加簇的数量会降低触发概率，而该概率用于解释在已知第一个模型中的某个簇的条件下，处于第二个模型的 M_2 簇之一的可能性。

图 10 展示了车辆在正常情况下（即不存在干扰器和欺骗器）、遭受干扰攻击以及遭受欺骗攻击时的轨迹示例。图中还显示了预测轨迹，该轨迹应遵循正常情况下学习到的相同动态规则。随后，我们在已学习的 C-GDBN 上实现 IM-MJPF，以进行多重预测，即预测路侧单元预期从某辆车辆接收到的射频信号，以及该车辆应遵循的相应轨迹。IM-MJPF 通过比较多重预测结果与观测值，生成式 (9) 和式 (10) 中定义的多个异常信号，用于检测干扰器和欺骗器。

图 11 展示了与图 10 所示示例相关的多种异常信号。可以观察到，在正常情况下，与射频信号（图 11-(a)）和轨迹（图 11-(b)）相关的异常信号均低于阈值。这证明路侧单元学会了在没有干扰器和欺骗器的情况下（即正常情况下）射频信号和轨迹如何演变的正确动态规则。此外，我们可以看到，路侧单元能够依靠异常信号，发现射频信号及其对应轨迹相对于迄今学到的内容因干扰而出现显著偏差。相比之下，在欺骗攻击下，路侧单元只会发现轨迹出现偏差，而射频信号没有偏差，因为欺骗器只影响了位置，并未操纵射频信号。此外，显而易见，所提出的方法使路侧单元能够识别所发生异常的类型，并解释检测到异常的原因（即判断异常是否由干扰器攻击 V2I 链路或欺骗器攻击卫星链路所致）。

图 12 展示了所提方法在多种情形下测试并

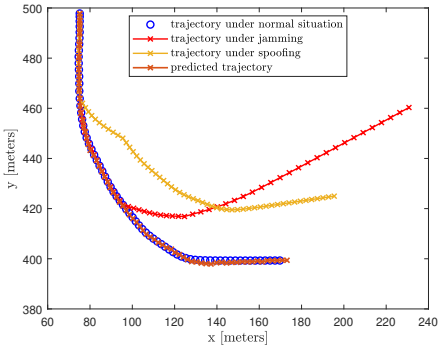

图 10. 正常情况下、受到干扰及遭受欺骗时车辆的轨迹。

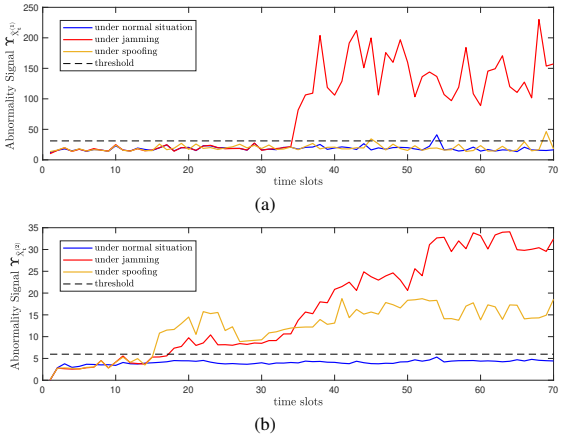

图 11. 与图 10 所示示例相关的异常信号：(a) 与射频信号相关的异常指标，(b) 与轨迹相关的异常指标。

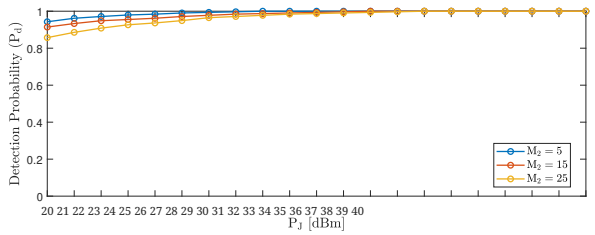

图 12. 使用不同簇数 M_2 时，检测概率 (P_d) 随干扰器功率 (P_J) 的变化。

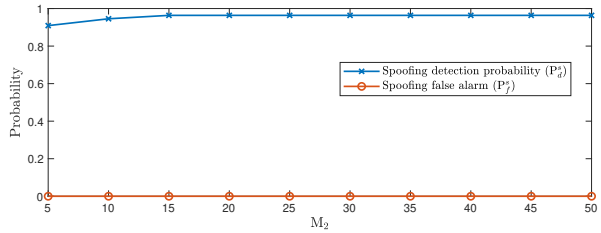

图 13. 欺骗检测概率 (P_d^s) 和欺骗虚警 (P_f^s) 随簇数 M_2 的变化。

通过考虑 20dBm 至 40dBm 范围内的不同干扰功率，检测干扰器的整体性能。可以看出，所提方法在考虑低功率和高功率干扰时，均能以很高的概率（接近 1）检测到干扰器。此外，该图还比较了簇数量变化时检测干扰器的性能（M_2）。图 13 展示了所提方法在测试不同驾驶操作示例时检测欺骗器的整体性能。可以看出，对于不同数量的簇，路侧单元均能以很高的检测概率且不产生虚警地检测到欺骗器。

V. 结论

本文提出一种联合检测GPS欺骗和干扰攻击的方法。该方法通过学习动态交互模型，编码来自多辆车的接收射频信号与其对应轨迹之间的互相关。仿真结果表明，所提出的方法在联合检测GPS欺骗器和干扰器攻击方面效果显著。后续工作将扩展系统模型，纳入两辆以上且信道条件各异、调制方案不同的车辆，以评估所提方法的有效性。

参考文献

[1] M. Noor-A-Rahim 等，“面向车联万物（V2X）通信的6G：赋能技术、挑战与机遇”，*IEEE* 论文集，第110卷，第6期，第712–734页，2022年6月。[2] S. Bartoletti 等，“面向5G及后续技术中车载安全应用的定位与感知”，*IEEE* 通信杂志，第59卷，第11期，第15–21页，2021年11月。[3] P. Gu 等，“车载网络中控制信道干扰的协作式抗干扰中继”，*IEEE* 车辆技术汇刊，第67卷，第8期，第7033–7046页，2018年8月。[4] N. Lyamin 等，“基于人工智能的VANET恶意网络流量检测”，*IEEE* 网络，第32卷，第6期，第15–21页，2018年11月。[5] C. Sanders和Y. Wang，“利用车际通信定位车辆GPS欺骗攻击”，*IEEE* 车辆技术汇刊，第69卷，第12期，第15 656–15 667页，2020年12月。[6] B. Yang 等，“基于欺骗相关峰抵消的全球导航卫星系统欺骗缓解技术研究”，*IEEE* 通信快报，第1–1页，2022年。[7] V. Sandeep 等，“混合射频与混合自由空间光通信/射频传输的车联网通信系统性能”，载于*IEEE*第*95*届车辆技术会议（*VTC2022-Spring*）论文集，2022年6月，第1–6页。[8] Y. Dang 等，“面向蜂窝连接无人机的基于深度集成学习的GPS欺骗检测”，*IEEE*物联网杂志，第1–1页，2022年。[9] N. Venkata Abhishek和M. Gurusamy，“JaDe：利用机器学习在车载网络中进行低功耗干扰检测”，*IEEE* 无线通信快报，第10卷，第10期，第2210–2214页，2021年10月。[10] C. Guo 等，“采用分组重传的高可靠、低时延车载通信资源分配”，*IEEE* 车辆技术汇刊，第68卷，第7期，第6219–6230页，2019年7月。[11] L. Liang 等，“车载通信中的基于图的资源共享”，*IEEE*无线通信汇刊，第17卷，第7期，第4579–4592页，2018年7月。[12] A. Krayani 等，“认知无人机无线电中的干扰信号自动分类”，*IEEE* 车辆技术汇刊，第1–17页，2022年。[13] B. Morris和M. Trivedi，“通过聚类学习轨迹模式：实验研究与比较评估”，载于*2009*年*IEEE*计算机视觉与模式识别会议，2009年6月，第312–319页。