深 圳 大 学

本 科 毕 业 论 文 (设计)

题目: 智能网联汽车 GNSS 位置欺骗攻击与功能安全危害联动预警策略设计及实现

姓名: 李宇良

专业: 计算机科学与技术

学院: 计算机与软件学院

学号: **2018151004**

指导教师: 肖志娇

职称: 副教授

2022 年 4 月 1 日

深圳大学本科毕业论文（设计）诚信声明

本人郑重声明: 所呈交的毕业论文 (设计), 题目《智能网联汽车 GNSS 位置欺骗攻击与功能安全危害联动预警 策略设计及实现》是本人在指导教师的指导下，独立进行研究工作所取得的成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式注明。除此之外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。本人完全意识到本声明的法律结果。

毕业论文（设计）作者签名:

日期:　　年　月　日

目　录

智能网联汽车 GNSS 位置欺骗攻击与功能安全危害联动预警策略设计及实现

计算机与软件学院计算机科学与技术专业　李宇良

学号：2018151004

【摘要】

【关键词】推荐系统; 协同过滤; 适应性采样

1 引言

1.1 研究背景及意义

近年来，随着现代通信技术以及自动驾驶技术的迅速发展，汽车这一传统出行载体也在往智能化、互联化的发展方向迈进。由此诞生出来的新产物便是智能网联汽车。区别于一般的自动驾驶汽车（ADAS），智能网联汽车可以理解为在自动驾驶技术的基础上（即自动驾驶决策单元、对应的传感器、控制器等），将车联网技术融合其中，使得汽车可以与周围环境、道路、甚至“云”，进行信息的沟通与共享，从而实现 V2X（Vehicle to X）[12]。这种互联化的技术可以使得传统自动驾驶汽车拥有更全面复杂的环境感知能力与决策能力，从而提高自动驾驶汽车的安全性与可靠性，并最终实现可以替代驾驶员所有操作的“无人驾驶汽车”。

外部网络接入带来的不仅有自动驾驶汽车各项能力的提升，随之而来的还有针对智能网联汽车的信息安全威胁。据国家工信部统计，自 2020 年以来，针对车联网信息服务提供商、整车企业等相关企业的恶意攻击高达 280 万起[7]；另外，截止到 2020 年底，全球范围内共发现 110 个与汽车产品相关的 CVE 漏洞。这些漏洞涉及范围广泛，包含汽车的内部网络、网关、传感器、车载信息娱乐系统、蓝牙、OBD 端口等等部件。这些针对汽车产品的安全漏洞以及攻击不仅会影响用户的信息娱乐服务质量，威胁用户的信息安全，甚至还很有可能导致汽车控制功能失效，直接威胁车内乘客的人身安全。由此可见，智能网联汽车相关的信息安全问题亟待解决。

一般而言，与智能网联汽车相关联的信息风险可以分为 IP 流量攻击风险，CAN 流量攻击风险，GNSS 位置欺骗攻击，蓝牙攻击风险以及车机攻击风险[10]。本文主要关注 GNSS 位置欺骗攻击，其中包括攻击检测以及对应功能安全危害的预警策略。

GNSS 位置欺骗攻击最早出现在军事领域。2011 年 12 月，伊朗使用 GNSS 位置欺骗攻击技术，成功控制了美军的 RQ-170 “哨兵”无人机，使其降落到伊朗机场。2016 年 1 月，美国海军的两艘小型巡逻艇在执行任务时偏离原本的航行路线，进入了伊朗海域，从而使船只与美国军方失去联系。而在民用领域，2014 年 3 月，从吉隆坡国际机场飞往北京首都机场的 MH370 航班在航行过程中失联，迄今尚未发现任何残骸。一些专家认为，MH370 很可能受到欺骗性的干扰，导致其偏离航线并在耗尽燃料后坠毁。从技术角度来看，GNSS 位置欺骗攻击确实具有这种潜在的攻击力[1]。近十年来，随着对该类攻击的深入研究，学术界已经有多种相对成熟的攻击检测方法。然而，这些研究大多数集中在军事领域，而由于军事设施与汽车在 GNSS 设备条件上的差异，这些成果往往不能直接应用到智能网联汽车上。而目前少部分聚焦于智能网联汽车 GNSS 位置欺骗研究的工作，往往仅关心 GNSS 位置欺骗攻击的检测方法，而忽略了攻击发生后可能会对汽车带来的功能安全危害，以及在攻击已经无法挽回的情况下如何采取应急策略来最小化损失。本文针对上述背景，提出了一种可以用于智能网联汽车 GNSS 位置欺骗攻击的检测方法，并在此基础上，提出相应的功能安全联动预警与应急策略，构建一个完整的“检测-预警-应急”系统。

1.2 本文主要工作

本论文分为六章，内容分别如下：

第一章为引言，主要介绍本论文的研究背景、研究意义、主要工作以及论文的组织结构。

第二章为相关技术简介，主要介绍与本论文工作相关的基础技术细节，包括 GNSS 原理概述，

LSTM 原理概述，汽车功能安全以及国内外对本文工作的研究现状。

第三章为基于 LSTM 进行汽车位置预测的 GNSS 位置攻击欺骗检测模型，介绍了如何基于 LSTM 构建一个可用于智能网联汽车的 GNSS 位置欺骗攻击检测算法。

第四章为 GNSS 位置欺骗攻击功能安全应急策略，主要介绍应对 GNSS 位置欺骗攻击的功能安全应急策略，以及如何将检测算法与应急策略进行联动。

第五章为实验与结果分析，主要介绍基于 CARLA 模拟器的仿真实验细节，以及具体的实验结果与分析。

第六章为结论与展望，主要是简要总结本文工作，并对进一步的研究工作提出展望。

1.3 本文贡献

2　相关技术简介

2.1　GNSS（全球卫星导航系统）概述

全球卫星导航系统（Global Navigation Satellite System, 下称 GNSS），一般是指通过覆盖全球的导航卫星系统为地面或近地面用户提供全天候的三维空间坐标以及时间信息的无线定位系统。使用 GNSS 进行定位的用户可以通过具有 GNSS 信号接收器接收来自当前区域卫星的定位信号，并通过一系列的解码与计算得到较为准确的空间信息与时间信息，从而实现定位、导航、授时（PNT）的功能。

世界上第一个全球卫星导航系统是美国的 GPS 系统。该系统在设计之初一共由 24 颗卫星组成，其中 21 颗为工作卫星，3 颗为备用卫星。而截至到目前，GPS 系统的卫星数目已经达到了 31 颗。而在我国，第一颗北斗卫星在 2007 年 4 月 14 日发射，被在往后的若干年里不断完善北斗导航系统。截至 2020 年，北斗系统已经实现向全球提供服务的目标，与美国 GPS、俄罗斯 GLONASS、欧盟 GALILEO 并列成为四大全球定位系统。除了上述的全球性定位系统外，还包括区域系统和增强系统。其中区域系统有日本的 QZSS 和印度的 IRNSS；增强系统则包括美国的 WASS、日本的 MSAS 以及欧盟的 EGNOS 等。

GNSS 的定位原理可以认为是求解一组方程。对于用户所处空间位置 (x_u, y_u, z_u)，由于导航卫星所处的精确位置是可知的，同时卫星与用户之间的距离也可通过光速与时间差得到，因此可以列出方程 (1)。

$$\rho_i = \|\mathbf{s}_i - \mathbf{u}\| \tag{1}$$

其中，ρ_i 则表示用户距离第 i 颗卫星的距离，$\mathbf{S}_i$ 表示第 i 颗卫星的空间位置，$\mathbf{U}$ 表示用户的空间位置。上述方程可展开为 (2)

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} \end{cases} \tag{2}$$

其中，x_i，y_i，z_i 表示当前用于定位用户位置的第 i 颗卫星的空间位置。求解上述方程组，即可求得用户位置坐标 (x_u, y_u, z_u)。然而，在实际应用中，除了上述的三个未知数以外，往往还需要第四个未知数 t_u 作为修正项。原因在于，在计算用户位置与卫星间距离时，需要使用导航卫星中的原子钟与地面用户接收器的时钟作差得到钟差，但接收器的时钟精度要比原子钟精度低。这就导致最终得到的钟差会有一定的误差，因此需要加入修正项。此时的方程如 (3) 所示。

$$\rho_i = \|\mathbf{s}_i - \mathbf{u}\| + ct_u \tag{3}$$

上式可展开为

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} + ct_u \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} + ct_u \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} + ct_u \\ \rho_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} + ct_u \end{cases} \tag{4}$$

其中，c 表示光速。

2.2 GNSS 位置欺骗攻击及检测方法概述

目前，GNSS 位置欺骗攻击还没有精确的定义。一般而言，“欺骗” 是指某人或某程序利用数据篡改、数据伪造等手段成功伪装成另一个人或另一个程序，其目的往往是获取情报或影响被攻击者的正常运作。具体到 GNSS 位置欺骗攻击方面，攻击者会通过伪造错误定位信号或转发真实卫星信号等手段进行攻击。遭受欺骗攻击的 GNSS 接收器则会计算出一个错误的位置或错误的时间，从而导致依赖于 GNSS 定位的其他部件工作受阻或出错，甚至是无法工作。下面将对常见的 GNSS 位置欺骗攻击手段及检测方法进行简要介绍。

2.2.1 欺骗方法概述

2.2.1.1 基于信号模拟器的自主产生式攻击 该攻击方式的主要思想是通过一个 GNSS 信号模拟器发送虚假 GNSS 定位信号来实现欺骗目的。目前，诸如 Spirent 公司的 GSS8000 等 GNSS 信号模拟器可以模拟出各种真实环境中的卫星定位信号。通过向接收机发送生成的定位信号的方法，可以实现一定程度上的位置欺骗攻击。但这种方法的缺点也很明显。由于 GNSS 信号模拟器所产生的信号是完全自主产生的，并没有与实际卫星进行信号同步，所以很容易导致接收机出现失锁或重捕的问题，从而导致欺骗被检测。另外，GNSS 模拟器庞大的体积以及高昂的价格也是该欺骗方法的主要缺点之一[11]。

2.2.1.2 基于接收机的接受产生式攻击 该攻击方式所使用的干扰源主要由两部分组成，即接收机与信号模拟器。接受产生式攻击的基本工作原理与自主产生式攻击类似，都需要使用一个信号模拟器进行信号模拟生产。两者最大的不同在于，前者在产生虚假定位信号时所使用的参数由操作者或机器自身自主设置；而后者则是根据接收机接收到的真是卫星信号的估计结果，通过算法计算得到。与自主产生式攻击相比，接收产生式攻击所产生的信号与真实信号接近，其隐蔽性要更强。而其缺点在于，由于在使用真实卫星信号计算模拟参数时需要精确测定目标接收机与欺骗干扰源之间的三维位置关系，实现难度较大。尤其是当欺骗目标处于运动状态的时候，需要实时测定两者位置关系。也正因如此，这种欺骗手段一般只用于静止状态或低速运动状态下的目标[11]。

2.2.1.3 基于信号转发器的转发式攻击 我国在 GNSS 欺骗方面的研究主要集中在转发式攻击。该攻击手段所采用的思路与上述两种欺骗方法截然不同。该方法不再生成虚假信号，而是直接使用真实的卫星导航信号，通过使用转发器发射到目标区域，从而使目标接收到另一个空间位置的 GNSS 定位信号。与产生式攻击方法相比，该方法最大的优点在于不需要了解信号的内部细节（如 GNSS 信号格式、加密方式等），从而避免了大量技术细节与限制，并因此扩大了适用范围。而该方法的最大缺点在于，由于在信号转发时需要对原始信号放大，这会导致信号中的噪声被一起放大，从而导致转发信号与接收机接收到的真实定位信号在噪声水平上有较大的差别，容易被检测到[11]。

2.2.2 检测方法概述

2.2.2.1 基于空间信息处理的检测方法 该检测方法的主要思想是通过判别导航信号的空间信息来实现欺骗检测。具体来说，GNSS 在定位时会从不同方向的不同卫星向用户发送定位信号；而欺骗源往往是从同一方向发射多个信号。通过处理接收到的信号，解算出信号的大致空间特征，就可以识别出当前收到的信号是否为欺骗信号。由于卫星的空间信息几乎是不可能被模仿的，因此这种检测方法是目前最为有效的 GNSS 欺骗检测方法之一[9]。

2.2.2.2 基于信号到达时间的检测方法 该检测方法的主要思想是通过判断欺骗信号与真实信号在到达时间上的差异来实现欺骗检测，主要用于转发式攻击。从2.2.1.3中可以看出，当使用欺骗设备对真实信号进行接收并转发后，目标接收机所接收到的信号必然会与真实信号在时间上有一定的延迟。根据这一特征，便可以判断当前是否收到了欺骗攻击。与转发式欺骗攻击方法一样，这种检测方法也是更适用于固定位置的接收机，在动态场景下的适用性有待提高[9]。

2.2.2.3 基于机器学习的检测方法 机器学习的方法也被应用到 GNSS 欺骗攻击检测中。举例而言，Semanjski S 等人[6] 将欺骗检测问题转化为分类问题，并使用 SVM 的方法来区分真实信号与欺骗信号，从而实现检测目的。L.Junzhi 等[4] 探讨了使用生成对抗网络（GAN）来进行 GNSS 欺骗检测的可行性；Dasgupta 等人[2] 将强化学习（Reinforcement Learning）的方法应用到 GNSS 的欺骗攻击检测中，通过使用来自自动驾驶汽车的 GNSS 定位信息、加速度、速度以及方向盘转向角，构建出一个可实现实时（turn-by-turn）欺骗检测的强化学习模型。

2.3 LSTM 概述

长短期记忆（LSTM）网络是深度学习领域处理序列问题的经典模型。该模型以传统的递归神经网络（RNN）为基础，通过增加细胞状态并引入门控电路（即输入门，输出门和遗忘门），有效解决了传统 RNN 在处理长序列问题时的依赖问题。LSTM 网络常被应用于序列问题，如机器翻译、文本生成、语音识别等。在本文中，由于汽车行驶的轨迹可以认为是连续序列，且轨迹点之间是有一定的关系与约束的，因此可以将 LSTM 网络应用到智能网联汽车的 GNSS 位置欺骗检测中。图1为 LSTM 网络结构。

在 LSTM 网络中，遗忘门的主要作用是控制当前细胞中信息的权重，并依次决定是否要舍弃信息。其计算公式如下：

$$f_i^{(t)} = \sigma\left(b_i^f + \sum_j U_{i,j}^f x_j^(t) + \sum_j W_{i,j}^f h_j^{(t-1)}\right) \tag{5}$$

其中，$\mathbf{x}^{(t)}$ 是当前输入向量，$\mathbf{h}^t$ 是当前隐藏层向量，其中包含所有 LSTM 细胞的输出。$\mathbf{b}^f$、$\mathbf{U}^f$、$\mathbf{W}^f$ 分别表示偏置、输入权重和循环权重。σ 表示 sigmoid 单元，作用是将权重设置为 0 到 1 之间的值。

输入门的作用主要是确定当前哪些细胞内的位置需要更新，并计算更新后的值。其计算公式如下所示：

$$g_i^{(t)} = \sigma\left(b_i^g + \sum_j U_{i,j}^g x_j^{(t)} + \sum_j W_{i,j}^g h_j^{(t-1)}\right) \tag{6}$$

其中，$\mathbf{x}^{(t)}$，$\mathbf{h}^t$ 分别表示当前输入向量与当前隐藏层向量；$\mathbf{b}^f$、$\mathbf{U}^f$、$\mathbf{W}^f$ 分别表示偏置、输入权重

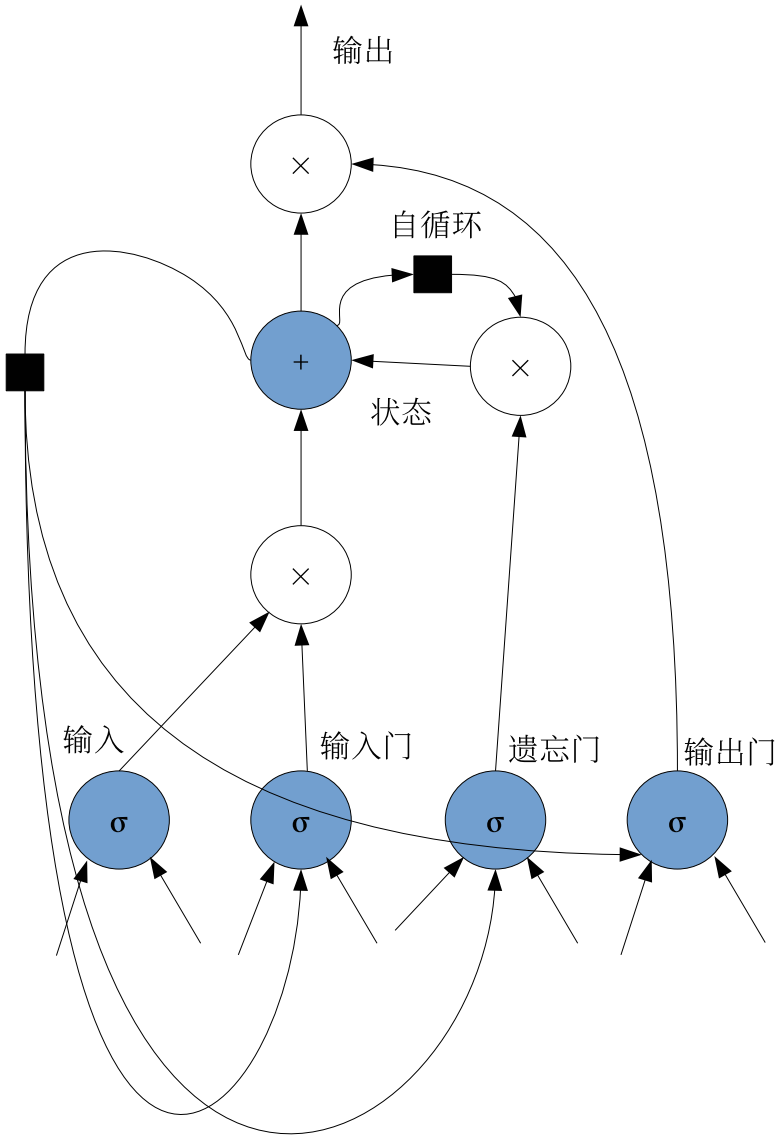

图 1: LSTM 网络结构图

和循环权重。在完成了输入门与遗忘门的计算后，LSTM 细胞内部参数会以下方式更新：

$$s_i^{(t)} = f_i^{(t)} s_i^{(t-1)} + g_i^{(t)} \sigma\left(b_i + \sum_j U_{i,j} x_j^{(t)} + \sum_j W_{i,j} h_j^{(t-1)} \right) \tag{7}$$

其中，$\mathbf{b}$、$\mathbf{U}$、$\mathbf{W}$ 分别表示 LSTM 细胞内的偏置、输入权重和循环权重。

最后，LSTM 会计算出最终隐藏层的输出。公式8计算出需要输出的细胞状态数值，公式9通过 tanh 函数将细胞状态处理为一个范围在 $(-1, 1)$ 内的数值。最后，$q_i^{(t)}$ 与 $h_i^{(t)}$ 相乘得到当前时刻隐藏层输出。

$$q_i^{(t)} = \sigma\left(b_i^o + \sum_j U_{i,j}^o x_j^{(t)} + \sum_j W_{i,j}^o h_j^{(t-1)} \right) \tag{8}$$

$$h_i^{(t)} = \tanh(s_i^{(t)}) q_i^{(t)} \tag{9}$$

其中，$\mathbf{b}^o$、$\mathbf{U}^o$、$\mathbf{W}^o$ 分别表示偏置、输入权重和输出权重。

2.4　汽车功能安全概述

汽车功能安全，一般是指在不存在电子或电气工程系统异常情况下所出现的不合理的危险[8]。与传统汽车相比，智能网联汽车的系统结构更复杂，大量应用了人工智能、协同计算等技术，这使得智能网联汽车的功能安全问题更为突出。目前学界对于功能安全的研究与开发一般遵循 ISO 26262 标准。该标准由 ISO 于 2011 年发布，其中主要包含了以下几点[3]：

1. 如何量化产品的安全等级；
2. 如何根据不同安全等级设计对应的安全措施；
3. 如何规避与控制系统性故障及随机故障；
4. 如何对功能安全进行管理。

另外，该标准中还提出了一种功能失效的危害分析与风险评估方法（Hazard Analysis & Risk Assessment，HARA），该方法被广泛应用到智能汽车软件开发行业中。具体而言，HARA 方法首先对汽车电子电气系统中可能存在的功能安全风险进行分析，然后在此基础上评估风险的严重度 S（Severity）、暴露度 E（Exposure）以及可控性 C（Controllabilit），最终确定各功能安全风险项的汽车安全完成性等级（Automotive Safetv Integration Level，ASIL）。表1展示了严重度、暴露度和可控性三个因子的划分标准；表2展示了通过 S、E、C 三个因子确定 ASIL 等级的依据。ASIL 等级由 A——D 表示，等级越高表示风险程度越高；QM（Quality Management）则表示质量管理，指只需要按照常规开发流程与质量管理体系进行开发即可，不需要增加额外的设计。

本文将参照 ISO 2626 标准，依据 HARA 功能安全分析方法，提出若干可用于响应 GNSS 位置欺骗攻击的功能安全应急策略，以实现检测算法与应急策略的联动。

严重度 S	暴露度 E	可控性 C
S0 无损害	E0 不可能	C0 一般可控制
S1 轻度或中度损害	E1 非常低的概率	C1 简单可控制
S2 严重损害	E2 低概率	C2 正常可控制
S3 致命损害	E3 中等概率	C3 难控制或不能控制
	E4 高概率	

表 1: HARA 方法中严重度、暴露度与可控性划分标准

严重程度	暴露概率	可控性		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

表 2: ASIL 划分标准

2.5 国内外研究现状

2.5.1 智能网联汽车 GNSS 位置欺骗攻击检测方面

2.5.1.1 国外研究现状 如2.2.2所述，GNSS 位置欺骗攻击检测所采取的方法一般有 i）基于空间信息处理的检测方法；ii）基于信号到达时间的检测方法；以及 iii）基于机器学习的检测方法。然而，这些方法并不一定完全适用于智能网联汽车。具体而言，

2.5.1.2 国内研究现状

2.5.2 智能网联汽车 GNSS 功能安全方面

2.6 本章小结

本章主要介绍了对本文所涉及到的技术做简要介绍。首先介绍了 GNSS 的工作原理、GNSS 位置欺骗攻击方法及检测方法；紧接着对 LSTM 网络的基本原理做了概述；接下来介绍了汽车功能安全的概念，以及相关的 ISO 26262 标准；最后，本章还就国内外学界就智能智能网联汽车 GNSS 欺骗检测以及功能安全方面的研究现状做了概述。

3　基于 LSTM 进行汽车位置预测的 GNSS 位置欺骗攻击检测算法

3.1　模型概述

如2.3所述，LSTM 作为传统 RNN 的改进模型，可以解决长序列问题中长期依赖的问题。对于本文中所涉及到的 GNSS 位置欺骗检测问题，由于汽车的移动轨迹可以看作是一个有依赖关系的连续序列，因此，可以使用 LSTM 作为问题的解决方案。模型的检测思路为，以被欺骗前目标车辆的 CAN 速度、IMU 前向加速度以及转向角作为输入，输出为下一时刻目标车辆所处位置与当前车辆位置之间距离的预测值 dis_p。计算 dis_p 与车辆实际移动距离 dis_g 的绝对值 dis_{abs}，并设置欺骗阈值 γ。若满足 $dis_{abs} > \gamma$，则认为此时目标车辆受到了 GNSS 位置欺骗。γ 的定义如下：

$$\gamma = \epsilon_{GNSS} + \epsilon_{LSTM} \tag{10}$$

其中，ϵ_{GNSS} 表示汽车 GNSS 模块定位误差，ϵ_{LSTM} 表示检测模型的预测误差。本文所使用的模型结构包括输入层、包含 50 个神经元的隐藏层以及输出层。如图2所示。

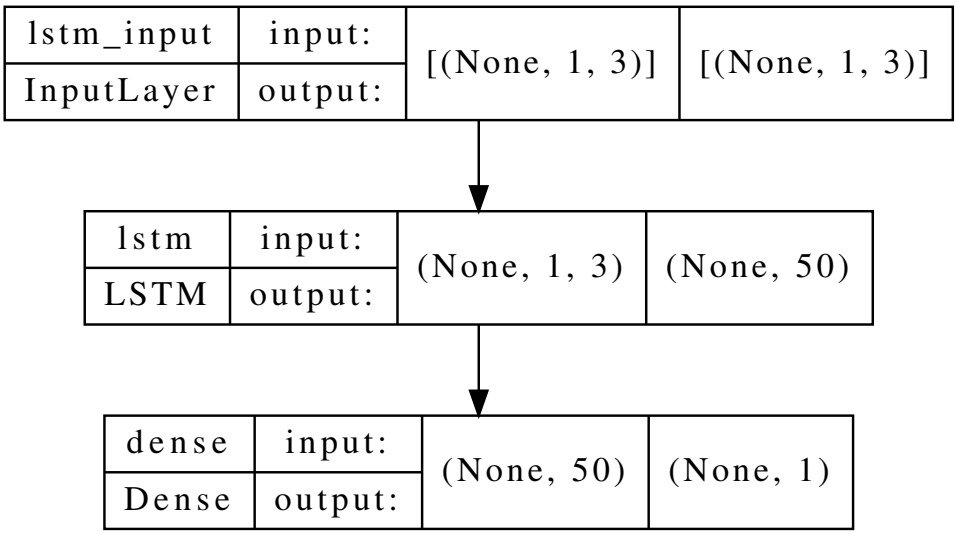

图 2: 本文所使用的 LSTM 模型结构

3.2　模型训练

本文在模型训练过程中将学习率设置为 0.01，batch size 设置为 64，并使用 Adam 优化器。另外，使用平均绝对误差（Mean Absolute Error，MAE）作为损失函数。MAE 的定义如公式 (11) 所示。

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|y_p - y_g| \tag{11}$$

其中，N 表示总样本数目，y_p 与 y_g 分别表示模型预测距离以及真实距离。模型训练过程中模型在训练集以及测试集的损失变化情况如图3所示。

紧接着，在模型训练完成后，以 RMSE 作为评价指标，并统计模型的最大误差、最小误差与平

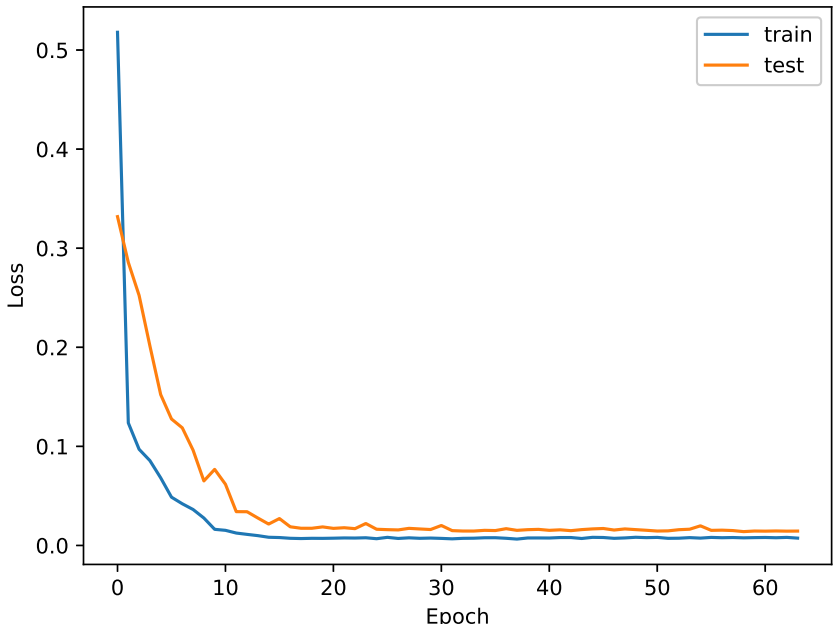

图 3: 平均绝对误差 (MAE)

评估指标	值
RMSE	0.072
min error	-0.000957(m)
max error	1.043058(m)
average error	0.070112(m)

表 3: 模型测试后统计得出的各评估指标

均误差，从而对模型的有效性进行评估。RMSE 计算公式如 (12) 所示。

$$RMSE = \frac{1}{N}\sqrt{\sum_{i=1}^{N}(y_p - y_g)^2} \tag{12}$$

其中，N 表示总测试样本数目，y_p 与 y_g 分别表示模型输出的预测距离与真实距离。所得出的评估结果如表 (3) 所示。

另外，为了直观呈现模型的有效性，图4展示了测试集上预测距离值与真实距离值的曲线图。从表 (3) 以及图4可以看出，模型的预测精确度较高，可以较好地实现 GNSS 位置欺骗攻击检测的目的。

3.3　GNSS 位置欺骗攻击检测

本文所采取的欺骗攻击检测方法，是通过比对上述模型的预测行驶距离与实际行驶距离来实现的。若两者间的差值大于误差阈值，则认为此时目标车辆受到了欺骗。检测算法伪代码见算法1。3.2中

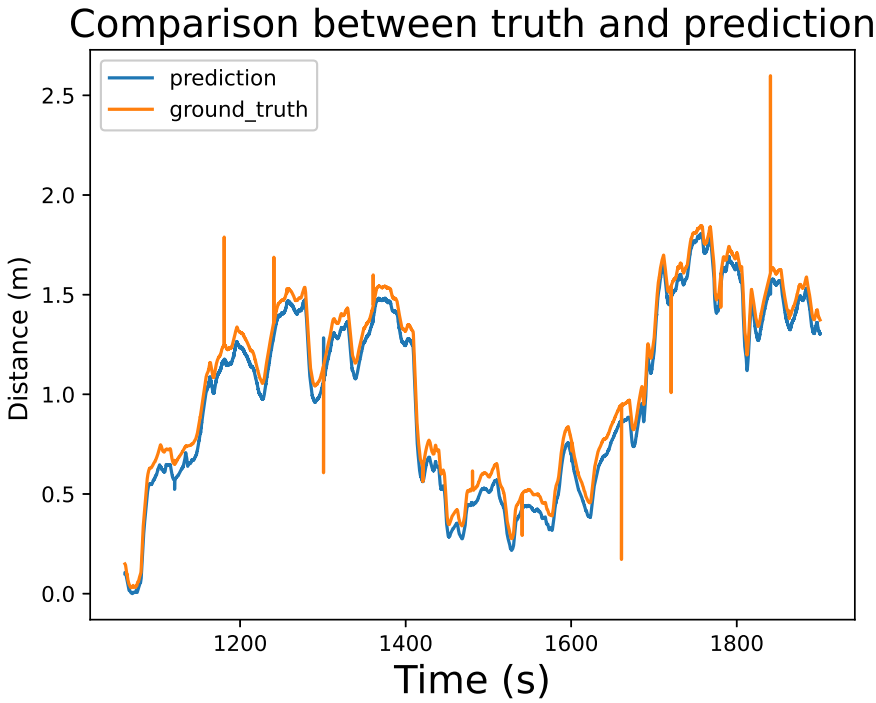

图 4: 预测距离值与真实距离值对比

定义欺骗阈值 $\gamma = \epsilon_{GNSS} + \epsilon_{LSTM}$。另外，由3.2可得知，模型的平均预测误差为 0.070112m；同时，由[5] 可知，目前常用的 GNSS 定位技术误差可认为是 10m。因此，有 $\gamma = 10 + 0.070112(m)$。

算法 1: GNSS 位置欺骗攻击检测算法

Input: 来自 CAN 的车速 v, 来自 IMU 的前向加速度 $a_{forward}$, 转向角 ω，来自 GNSS 模块的实际行驶距离 dis_{truth}，行驶距离预测模型 M，欺骗阈值 γ

Output: 表示是否受到欺骗的布尔值 $spoofed$

$dis_{predict} = M(v, a_{forward}, \omega)$;
if $\|dis_{predict} - dis_{truth}\| > \gamma$ **then**
    $spoofed \leftarrow True$;
else
    $spoofed \leftarrow False$;
end
return $spoofed$;

3.4 本章小结

本章主要介绍了基于 LSTM 的智能网联汽车 GNSS 位置欺骗攻击检测算法的基本思路、模型结构以及训练细节。同时通过 MAE 与 RMSE 说明了模型的有效性。

4　GNSS 位置欺骗攻击功能安全应急策略

4.1　策略描述

4.2　策略与检测模型联动

4.3　本章小结

5　实验与结果分析

5.1　训练数据集概述与数据处理

5.2　攻击生成

5.3　基于 CARLA 的仿真实验验证

5.4　本章小结

6　结论与展望

6.1　结论

6.2　进一步研究工作

【参考文献】

[1] BIAN, S., HU, Y., and JI, B. (2017). Research status and prospect of gnss anti-spoofing technology. *Scientia Sinica Informationis*, 47(3):275–287.

[2] Dasgupta, S., Ghosh, T., and Rahman, M. (2021). A reinforcement learning approach for gnss spoofing attack detection of autonomous vehicles. *arXiv preprint arXiv:2108.08628*.

[3] ISO (2018). Iso 26262-1:2018.

[4] Junzhi, L., Wanqing, L., Qixiang, F., and Beidian, L. (2019). Research progress of gnss spoofing and spoofing detection technology. In *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pages 1360–1369.

[5] Kaplan, E. and Hegarty, C. (2005). *Understanding GPS: Principles and Applications*. Artech House mobile communications series. Artech House.

[6] Semanjski, S., Semanjski, I., De Wilde, W., and Gautama, S. (2020). Gnss spoofing detection by supervised machine learning with validation on real-world meaconing and spoofing data-part ii. *Sensors (Basel, Switzerland)*, 20(7).

[7] 中国软件评测中心·智能网联汽车测评工程技术中心 (2021). 智能网联汽车安全渗透白皮书 2.0.

[8] 刘法旺 and 李艳文 (2021). 自动驾驶系统功能安全与预期功能安全研究. 工业技术创新, 8(3):7.

[9] 周彦, 王山亮, 杨威, 张世仓, and 蔡成林 (2022). Gnss 欺骗式干扰检测综述. 计算机工程与应用, page 12.

[10] 宋昊辰, 杨林, 徐华伟, 杨珺婕, 胡坚耀, and 陈超英 (2020). 智能网联汽车信息安全综述. 信息安全与通信保密, (7):9.

[11] 庞晶, 倪少杰, 聂俊伟, and 欧钢 (2016). Gnss 欺骗干扰技术研究. 火力与指挥控制, 41(7):5.

[12] 郝晶晶 and 韩光省 (2021). 智能网联汽车信息安全威胁识别和防护方法研究. 现代电子技术, 44(23):5.

致谢

Research on Content-Aware Collaborative Filtering

【Abstract】 Pairwise learning algorithms are a vital technique for personalized ranking with implicit feedback. They usually assume that each user is more interested in items which have been selected by the user than remaining ones. This pairwise assumption usually derives massive training pairs. To deal with such large-scale training data, the learning algorithms are usually based on stochastic gradient descent with uniformly drawn pairs. However, the uniformly sampling strategy often results in slow convergence. In this paper, we first uncover the reasons of slow convergence. Then, we associate contents of entities with characteristics of dataset to develop an adaptive item sampler for drawing informative training data. In this end, to devise a robust personalized ranking method, we accordingly embed our sampler into Bayesian Personalized Ranking (BPR) framework, and further propose a Content-aware and Adaptive Bayesian Personalized Ranking (CA-BPR) method, which can model both contents and implicit feedbacks in a unified learning process. The experimental results show that our adaptive item sampler can indeed improve recommendation performance.

【Keywords】 Recommendation System; Collaborative Filtering; Adaptive Sampling

指导教师: 潘微科