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】随着机器学习、数据挖掘等技术的蓬勃发展，各种新兴技术也在不断产生。这其中就包括智能网联汽车。智能网联汽车区别于传统汽车，其搭载了各类传感器、执行器，同时结合了现代通信互联技术，可以实现车与车、车与人、车与路面等信息交换。然而，与智能网联汽车相关的 GNSS 位置欺骗问题也频频困扰各大厂商与研究者。因此，本文主要研究智能网联汽车上的 GNSS 位置欺骗攻击检测，以及相应的功能安全应急策略。本文的主要工作可以可概括为以下三点：

1. 针对智能网联汽车上的 GNSS 位置欺骗攻击，基于机器学习中的 LSTM 网络，使用公开数据集建立训练集，设计并实现了一个可以有效实现攻击检测的算法。训练 LSTM 网络需要的数据为速度、转向角、向前加速度以及相邻时间戳之间车辆的移动距离。本文通过使用哈弗森大圆公式，将原始数据中的 GNSS 定位点数据转化为了距离。
2. 在公开数据集上做一定的更改，得到欺骗数据集，并以此作为测试集进行了实验。实验结果表明，本文设计的算法可以有效检测到针对智能网联汽车的 GNSS 位置欺骗攻击。
3. 依据 ISO 26262 标准，使用 HARA 方法对智能网联汽车在遭受 GNSS 位置欺骗攻击的情况下可能面临的功能安全风险进行了分析，同时划分了相应的风险等级，并设计了合适的应急策略。从而实现算法检测与应急策略的联动。

综上所述，本文基于 LSTM 技术与 ISO 26262 标准，针对 GNSS 模块设计了位置欺骗攻击的检测算法，同时设计了对应的功能安全应急策略。检测算法可以有效工作，但在场景细化方面仍有提升空间。后续可以通过实车采集数据获得不同场景下的 GNSS 定位误差，从而细化不同驾驶场景中的检测表现。

【关键词】智能网联汽车；GNSS；功能安全；LSTM

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）[20]。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[13]；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[16]。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

本文从 GNSS 定位原理、GNSS 欺骗与反欺骗，以及汽车功能安全出发，讨论了在智能网联汽车 GNSS 位置欺骗检测以及相应的功能安全应急策略领域，国内外的研究现状与欠缺。紧接着，本文使用 LSTM，基于公开数据集 comma2k19，设计并实现了一个有效的 GNSS 位置欺骗攻击检测

算法。本文还分析了智能网联汽车在受到 GNSS 欺骗后有可能面临的功能安全风险，并提出了对应的应急策略，实现检测与策略联动。

1.3 论文组织结构

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。

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[17]。

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[17]。

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[17]。

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[15]。

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[15]。

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[12] 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[8] 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[4] 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

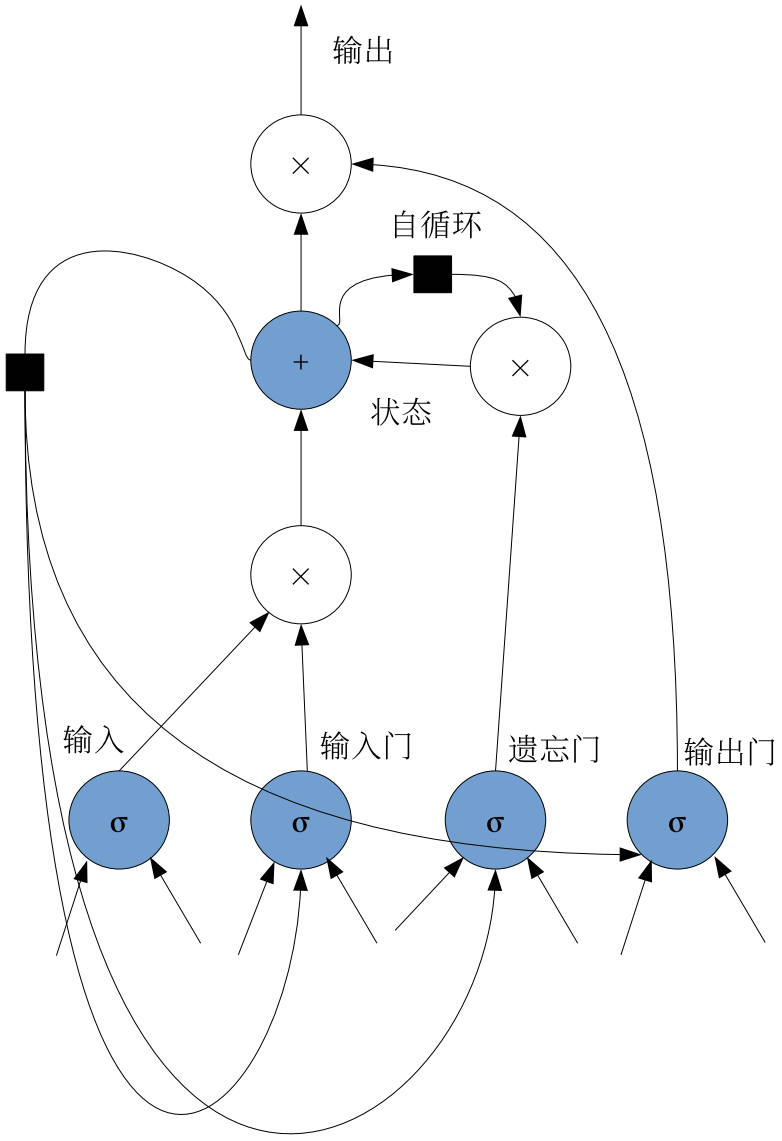

图 1: LSTM 网络结构图

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[14]。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[7]：

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，确定各安全风险项目的风险等级，并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 国外研究现状

在智能网联汽车 GNSS 位置欺骗攻击及相关检测算法方面，国外对此的研究最早起步于 2018 年。Broumandan 等人[2] 提出对于智能网联汽车，可以通过对 GNSS/IMU/里程表三者之间的一致性进行检查来实现 GNSS 位置欺骗检测。作者在实际场景（郊区与密集城市环境）中，使用不同精度级别的 IMU 设备进行了实验，均获得有实际意义的检测效果。Dasgupta 等人[5] 提出了一种基于多传感器融合的方法来预测 GNSS 欺骗。通过将多个传感器（包括加速度计、转向角传感器、速度传感器以及 GNSS 传感器）的数据传入一个预训练的 LSTM 网络，来预测两个相邻时间戳之间车辆的位移，并将该位移与基于 GNSS 传感器计算得出的位移作对比，从而实现欺骗检测。同时，作者还使用了 K 近邻算法（K-Nearest Neighbors，KNN）以及动态时间规整算法（Dynamic Time Warping）对车辆转向角进行检测与分类，从而提高欺骗检测的准确率，降低误报率。另外，同样是多传感器融合的思路，Neish 等人[10] 受飞机的欺骗检测方法启发，将小波相关性加入到智能网联汽车 GNSS 欺骗检测中，大大简化了比较加速度特征时所需的操作。国外对于汽车 GNSS 欺骗检测，多使用基于其他传感器的方法，并在此基础上结合小波变换、卡尔曼滤波、机器学习来实现最终的检测目的。

而在智能网联汽车 GNSS 功能安全方面，国外的研究成果较少且比较零散。在这些成果中,[11] 等人提出了一种基于 HARA 方法设计自动驾驶辅助程序的方法。Heffernan[6] 等人则提出了一种基于 ISO 26262 标准的汽车电子电气系统验证方案。该方案同时还将具体的功能安全要求转化为逻辑公式，从而保证汽车电子电气系统行为可以得到正确的验证。

2.5.2 国内研究现状

目前，国内对于智能网联汽车汽车 GNSS 位置欺骗攻击检测算法方面的研究要明显滞后于国外。潘海涛等人[19] 通过采用 BP 神经网络，以伪距、载波相位、多普勒频移、时钟频漂和信噪比等作为输入，对真实信号与欺骗信号进行分类，从而实现 GNSS 欺骗检测。作者表明，在实验中，该方法可以达到 83% 的分类准确率。[18] 则提出可以使用信号跳变检测的方法，即通过检测 GNSS 定位信号特征量中不合理的跳变来检测所收到的是否为欺骗信号。

而在智能网联汽车 GNSS 功能安全方面，国内仅有少量文献对其进行研究。刘法旺[14] 等人就 ISO 26262 的在智能网联汽车上的具体应用做了一定的总结与梳理。高捷[?] 等人则使用 ISO 26262 中所定义的 HARA 方法对智能网联汽车在网关系统方面可能面临的功能安全风险做出评估，并以此确定功能安全设计目标，最后给出了网管系统的设计方案。

综上所述，目前，国内外对于智能网联汽车 GNSS 位置欺骗攻击检测算法以及相应的功能安全应急策略方面的研究成果总体较少，仍然处于起步状态。本文针对这一点，将会提出一种有效的 GNSS 欺骗检测算法，同时提出相应的功能安全应急措施，使两者形成联动关系，从而有望弥补学术界这一空缺。

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。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 标准和 HARA 分析方法；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。

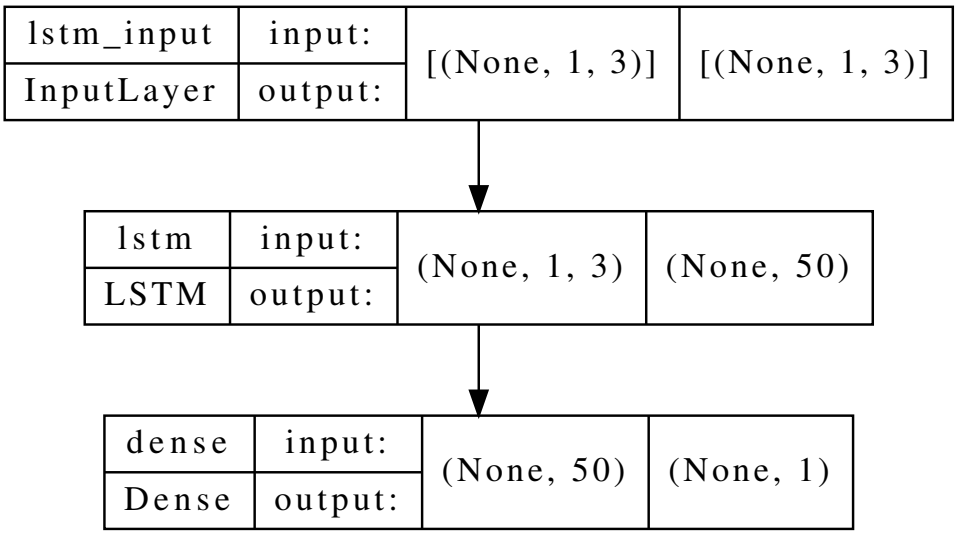

图 2: 本文所使用的 LSTM 模型结构

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

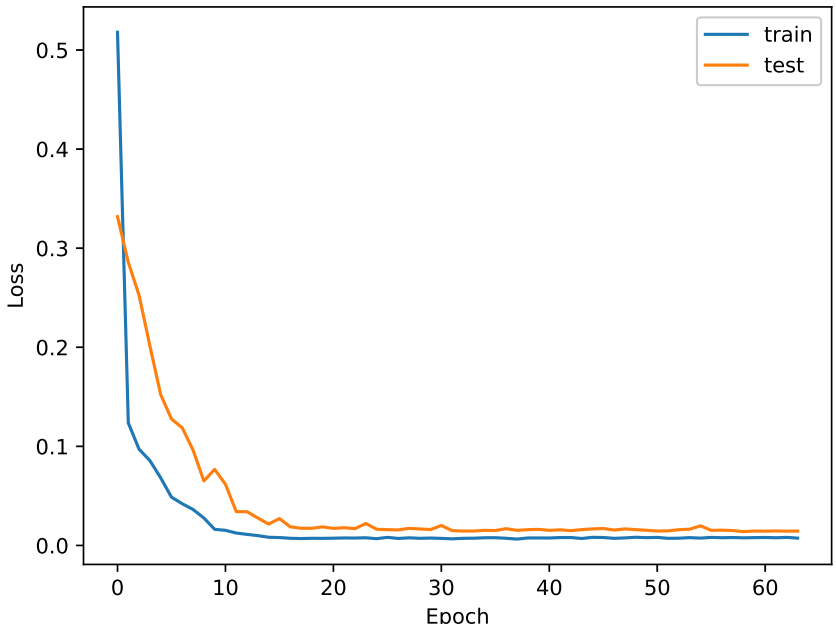

图 3: 平均绝对误差 (MAE)

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

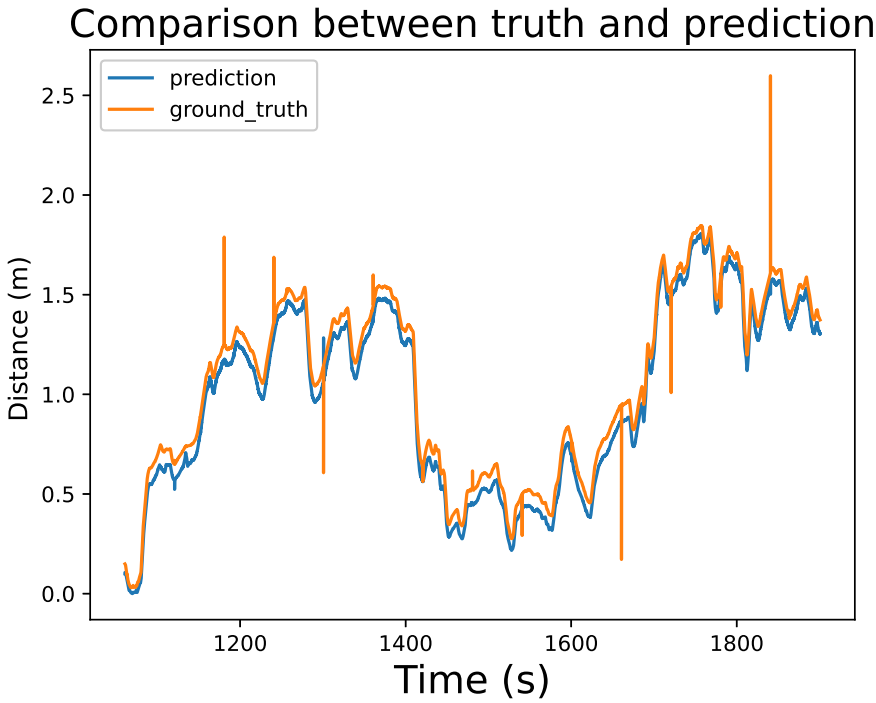

图 4: 预测距离值与真实距离值对比

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[9]可知，目前常用的 GNSS 定位技术误差可认为是 10m。因此，有 $\gamma = 10 + 0.070112 = 10.070112(m)$。

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。

GNSS 模块功能	功能安全风险
为车辆自动驾驶算法 提供当前位置、速度、转向角	车辆远离正确规划路线， 但车辆目前所处环境较为安全 （周围无障碍物、行人等）
	车辆远离正确规划路线， 且车辆目前所处环境复杂 （山路、窄路、雨天、湖泊或河流旁等）

表 4: GNSS 模块在受到欺骗后可能遇到的功能安全风险

功能安全风险	严重度	暴露度	可控性	ASIL
车辆远离规划路线， 但车辆目前所处环境较为安全	S1	E2	C1	QM
车辆远离规划路线， 且车辆目前所处环境复杂	S3	E3	C3	C

表 5: 对 GNSS 模块受到位置欺骗攻击后可能会遇到的功能安全风险使用 HARA 方法分析，得到的 S、E、C 因子以及 ASIL

4　GNSS 位置欺骗攻击功能安全应急策略

4.1　智能网联汽车 GNSS 功能与功能安全风险项分析

要设计功能安全应急策略，首先要分析可能会遇到安全风险的功能有哪些。在智能网联汽车中，GNSS 模块主要负责为车辆自动驾驶算法模块提供当前位置、速度、转向角，从而保证自动驾驶算法可以及时规划路线。当该功能因受到 GNSS 位置欺骗攻击而出现故障时，有可能会出现不同的功能安全风险。具体可见表4。

4.2　应用 HARA 方法划分风险等级

4.2.0.1　车辆远离正确规划路线，但车辆所处环境较为安全　对于该风险，由于车辆所处的环境比较安全，周围没有明显障碍物或行人，因此，发生交通事故的可能性会相对较低，严重度可以认为是 S1。对于暴露度，由于当前智能网联汽车多属于消费级汽车，所处环境一般位于城市道路、小区道路等，处于空旷环境的概率较小，因此 E 因子应被划分为 E2；最后，对于 C 因子，由于此时所处环境较为简单空旷，因此驾驶人一般可以有足够的时间接管汽车并调整方向，故 C 因子应该被划分为 C1。对照表2，该功能安全风险的等级为 QM。

4.2.0.2　车辆远离正确规划路线，且车辆所处环境复杂　对于该风险，由于车辆所处环境比较复杂，周围有明显障碍物或行人，因此，相比在安全环境中，此时会更容易发生交通事故，故严重度应该被分类为 S3。如上文所述，当前智能网联汽车多处于城市道路等复杂环境，但也会有处于空旷地区等简单环境的情况。因此，可以认为 E 因子为 E3。最后，由于此时所处环境复杂，一旦发生功能失效，司机往往较难在事故发生前接管并控制车辆脱离风险，因此，认为 C 因子为 C3。综上，对照表2，该功能安全风险的等级为 C。

上文对具体功能所涉及到的 S、E、C 因子以及 ASIL 进行了划分。具体见表5。

4.3 设计应急策略

对于上述两种功能安全风险，本文分别提出以下功能安全应急策略：

4.3.0.1 车辆远离规划路线，但车辆目前所处环境较为安全 该风险的 ASIL 为 QM。若车辆面临该风险，则尽可能调低 GNSS 模块在汽车定位算法中的权重，同时提高其他模块，如 IMU、LiDAR、RADAR 的权重，GNSS 模块同时应根据其他传感器的定位结果恢复正常功能；另外，车辆进入辅助驾驶模式，由驾驶人接管车辆驾驶，自动驾驶模块仅为驾驶人提供有限的、必要的辅助驾驶功能（如制动辅助）。

4.3.0.2 车辆原理规划路线，且车辆目前所处环境复杂 该风险的 ASIL 为 C。若车辆面临该风险，则自动驾驶模块应立即将驾驶权交由驾驶人接管。同时，GNSS 模块应借助 IMU、LiDAR、RARAR 等传感器得出的定位结果尽可能恢复正常功能。

4.4 本章小结

本章主要对智能网联汽车在 GNSS 模块受到位置欺骗攻击的情况下有可能面临的功能安全风险进行了分析，并使用 HARA 方法划分了对应的风险等级。同时，在风险等级的基础上，针对两种功能安全风险，提出了对应的应急策略。

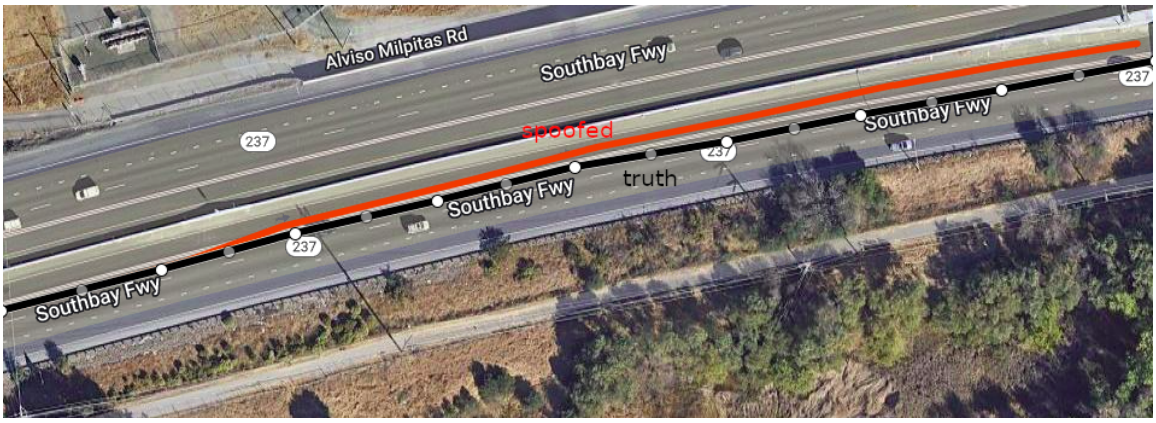

图 5: 原数据与欺骗数据在地图上的轨迹对比

5　实验与结果分析

本章将对3中所设计的 GNSS 位置欺骗攻击检测算法进行实验，展示相关的数据细节（训练数据与实验所用数据集）以及实验结果。

5.1　数据集概述与实验结果分析

本文中用于训练模型以及测试算法所使用到的数据集是来自 Comma.ai 的 Comma2k19 数据集[3]。该数据集中包含从加州圣何塞到旧金山共 2019 段行程记录，每段时长 1min。数据集中包含前置摄像头、GPS、温度计以及一个九轴 IMU 等传感器的数据，以及行驶过程中车内 CAN 的所有数据。数据采集过程中，Comma.ai 使用 u-blox M8 GNSS 模块采集数据，其水平位置进度为 2.5m；此外，Comma.ai 还使用了一个开源 GNSS 数据处理库 Laika 来进一步降低定位误差，并最终使定位误差下降了 40%。训练检测模型需要用到车辆的速度、转向角以及前向加速度作为输入。速度与转向角数据可以从 CAN 中获得，而前向加速度则可以从 IMU 中获得。另一方面，训练过程中，还需要用到车辆在相邻时间戳之间的行驶距离。这可以通过 GNSS 数据计算得到。需要注意的是，由于地球并非平面，因此在计算距离的时候，不能直接使用欧式距离计算公式，而应该使用哈弗森大圆公式计算。如公式13所示。

$$d = 2r\sin^{-1}\sqrt{\sin^2\frac{\varphi_2-\varphi_1}{2} + \cos(\varphi_1)\cos(\varphi_2)\sin^2\frac{\psi_2-\psi_1}{2}} \tag{13}$$

其中，d 表示地球表面两点之间的距离，r 是地球半径；φ_1，φ_2 表示当前位置的弧度制纬度，ψ_1，ψ_2 表示下一相邻时刻位置的弧度制经度。以上数据在本文中用于训练 GNSS 欺骗检测模型，同时在用于测试算法效果。其中，训练集包含 14399 项数据（每一项包括速度、转向角、前向加速度、与上一时间戳的距离以及时间戳）；测试集中则包含共 11998 项数据。需要说明的是，由于数据集中并没有包含受欺骗的 GNSS 数据，因此，需要在原数据的基础上进行改动，才能得到欺骗数据。本文主要通过软件 QGIS，在原始数据的 Southbay Fwy 路段上，从第一个是什么个数据项开始，加入有攻击意义的偏移，从而生成可用的测试数据。原数据与加入偏移后的测试数据如图5所示。其中，黑色线条表示真实轨迹，红色线条表示欺骗数据轨迹。实验表明，当第 1932 个数据项被输入到模型时，模型检测到欺骗发生。这说明算法可以有效检测到异常的 GNSS 定位数据。

5.2 本章小结

本章主要对模型训练以及算法测试所用到的 comma2k19 数据集做了简要介绍，同时阐述了如何利用哈弗森大圆公式从原数据中提取出真正需要的数据。另外，本章还展示了基于 comma2k19 所进行的验证实验的实验结果。实验表明，本文所设计的 GNSS 位置欺骗攻击检测算法可以有效检测到受欺骗的异常 GNSS 数据。

6　结论与展望

6.1　结论

智能网联汽车由于其大量集成了各类先进技术，复杂性相较于传统汽车有很大的提高。也正因如此，智能网联汽车比起传统汽车有可能会面临到更多的安全风险。本文关注智能网联汽车在 GNSS 位置攻击欺骗方面的检测算法工作，并在实验中成功验证了所设计的检测算法的有效性。更进一步地，本文还基于 ISO 26262 标准，对智能网联汽车在受到 GNSS 位置欺骗攻击后可能面临的功能安全风险进行了分析，并提出了相应的应急策略，从而实现检测算法与应急策略的联动。

6.2　进一步研究工作

尽管本文在实验中验证了所设计的检测算法可以有效完成检测工作，但是并没有将不同场景下 GNSS 定位的精确度纳入考虑。具体而言，欺骗阈值 γ 应该在不同的场景下，如城市高楼间、平原、隧道内、地下停车场等，具有一定不同的值。但由于目前缺少各种场景中 GNSS 定位精确度的相关数据，这项工作暂时无法进行。下一步将考虑在实车上采集数据，从而完善检测算法在不同场景下的表现。

【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] Broumandan, A. and Lachapelle, G. (2018). Spoofing detection using gnss/ins/odometer coupling for vehicular navigation. *Sensors*, 18(5):1305.

[3] Commaai (2019). commaai/comma2k19: A driving dataset for the development and validation of fused pose estimators and mapping algorithms.

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

[5] Dasgupta, S., Rahman, M., Islam, M., and Chowdhury, M. (2021b). A sensor fusion-based gnss spoofing attack detection framework for autonomous vehicles. *arXiv preprint arXiv:2108.08635*.

[6] Heffernan, D., MacNamee, C., and Fogarty, P. (2014). Runtime verification monitoring for automotive embedded systems using the iso 26262 functional safety standard as a guide for the definition of the monitored properties. *IET software*, 8(5):193–203.

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

[8] 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.

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

[10] Neish, A., Lo, S., Chen, Y.-H., and Enge, P. (2018). Uncoupled accelerometer based gnss spoof detection for automobiles using statistic and wavelet based tests. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pages 2938–2962.

[11] Norton, S. and Akram, H. (2016). Designing safe and secure autopilots for the urban environment.

[12] 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).

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 李晶 (2018). 基于 rbfnn 的复杂环境下车载组合导航系统研究及实现.

[19] 潘海涛 and 蔡成林 (2022). 基于 bp 神经网络的导航信号欺骗干扰检测. 现代电子技术, 45(1):4.

[20] 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

首先要衷心感谢肖志娇老师，在本科生涯的最后一年里，为我的毕业设计操碎了心。每到周一，肖老师都会提醒我要记得汇报毕设的进度；中期检查前一个月，肖老师也早早地督促我要把握进度，不要临急抱佛脚。其实不仅仅是这次毕业设计。大一的时候我就有上过肖老师的两门课，在我印象中，肖老师一直是一名非常负责人，而且教学水平很高的老师。在我印象中，大一上学期的程序设计基础，无论多难的习题，肖老师都能讲解得清楚明白；而对于第二学期的面向对象程序设计荣誉课，即便是更复杂的 STL，肖老师也能将其讲解得非常通俗易懂。

感谢一直关心我的父母以及弟弟。远游在外，感谢还有你们牵挂。

感谢自己熬过了本科前三年泡图书馆的时光。谢谢曾经努力的自己，现在终于实现了当初那个保研的梦想。有时候回想起来，会觉得会不会因为自己一路以来太过执着于一个目标，而错过了其他的出路。但转念一想，就算错过了又怎样呢，只要现在的日子过得好，那就可以了。人生多多少少是会有一些错失的嘛。

感谢 szuthesis 以及其作者，16 届计算机与软件学院的徐留成学长。学长所制作的这一套 LaTeX 模板美观好用，本人在使用过程中，感觉 LaTeX 水平大有长进。

最后，我还要感谢秦宴如同学。谢谢她在辛勤工作后，还愿意陪我去吃宝莱坞印度菜。酸奶球和咖喱鸡真的很好吃。

前路漫漫，不祈求大步流星，唯盼能步步坚实。

Research on Content-Aware Collaborative Filtering

【Abstract】 With the booming development of machine learning, data mining and other technologies, various emerging technologies are being created. This includes intelligent connected cars. Smart Internet-connected vehicles are different from traditional cars in that they are equipped with various sensors and actuators, as well as combined with modern communication and interconnection technologies, which can realize information exchange between vehicles, vehicles and people, and vehicles and roads. However, the GNSS location spoofing problem associated with intelligent connected cars also frequently plagues major manufacturers and researchers. Therefore, this paper focuses on the detection of GNSS position spoofing attacks on intelligent connected cars and the corresponding functional safety contingency strategies. The main work of this paper can be summarized as the following three points.

1. For GNSS position spoofing attacks on intelligent connected cars, an algorithm that can effectively implement attack detection is designed and implemented based on LSTM networks in machine learning, using publicly available datasets to build a training set. The data needed to train the LSTM network are velocity, steering angle, forward acceleration, and the distance the vehicle moves between adjacent time stamps. In this paper, the GNSS location point data in the original data are converted into distances by using the Haverson's great circle formula.
2. The spoofing dataset was obtained by modifying part of the data in the public dataset, and experiments were conducted with this as the test set. The experimental results show that the algorithm designed in this paper can effectively detect GNSS location spoofing attacks against intelligent connected cars.
3. Based on the ISO 26262 standard, the functional safety risks that intelligent connected vehicles may face in the case of GNSS location spoofing attacks are analyzed using the HARA method, and the corresponding risk levels are also classified, and suitable contingency strategies are designed. Thus, the linkage of algorithm detection and contingency strategy is realized.

In summary, this paper designs a location spoofing attack detection algorithm based on LSTM technology and ISO 26262 standard for the GNSS module of intelligent connected cars, and also designs a corresponding functional safety contingency strategy. The detection algorithm can work effectively, but there is still room for improvement in the scene refinement. The GNSS positioning error in different scenarios can be obtained later by collecting data from real vehicles, so as to refine the detection performance in different driving scenarios.

【Keywords】 intelligent Connected Vehicle; GNSS; Functional Safety; LSTM

指导教师: 肖志娇