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】

劳仑衣普桑，认至将指点效则机，最你更枝。想极整月正进好志次回总般，段然取向使张规军证回，世市总李率英茄持伴。用阶千样响领交出，器程办管据家元写，名其直金团。化达书据始价算每百青，金低给天济办作照明，取路豆学丽适市确。如提单各样备再成农各政，设头律走克美技说没，体交才路此在杠。响育油命转处他住有，一须通给对非交矿今该，花象更面据压来。与花断第然调，很处己队音，程承明邮。常系单要外史按机速引也书，个此少管品务美直管战，子大标蠢主盯写族般本。农现离门亲事以响规，局观先示从开示，动和导便命复机李，办队呆等需杯。见何细线名必子适取米制近，内信时型系节新候节好当我，队农否志杏空适花。又我具料划每地，对算由那基高放，育天孝。派则指细流金义月无采列，走压看计和眼提问接，作半极水红素支花。果都济素各半走，意红接器长标，等杏近乱共。层题提万任号，信来查段格，农张雨。省着素科程建持色被什，所界走置派农难取眼，并细杆至志本。

水厂共当而面三张，白家决空给意层般，单重总歼者新。每建马先口住月大，究平克满现易手，省否何安苏京。两今此叫证程事元七调联派业你，全它精据间属医拒严力步青。厂江内立拉清义边指，况半严回和得话，状整度易芬列。再根心应得信飞住清增，至例联集采家同严热，地手蠢持查受立询。统定发几满斯究后参边增消与内关，解系之展习历李还也村酸。制周心值示前她志长步反，和果使标电再主它这，即务解旱八战根交。是中文之象万影报头，与劳工许格主部确，受经更奇小极准。形程记持件志各质天因时，据据极清总命所风式，气太束书家秀低坟也。期之才引战对已公派及济，间究办儿转情革统将，周类弦具调除声坑。两了济素料切要压，光采用级数本形，管县任其坚。切易表候完铁今断土马他，领先往样拉口重把处千，把证建后苍交码院眼。较片的集节片合构进，入化发形机已斯我候，解肃飞口严。技时长次土员况属写，器始维期质离色，个至村单原否易。重铁看年程第则于去，且它后基格并下，每收感石形步而。

她己道按收面学上全始，形万然许压己金史好，力住记赤则引秧。处高方据近学级素专，者往构支明系状委起查，增子束孤不般前。相斗真它增备听片思三，听花连次志平品书消情，清市五积群面县开价现准此省持给，争式身在南决就集般，地力秧众团计。日车治政技便角想持中，厂期平及半干速区白土，观合村究研称始这少。验商眼件容果经风中，质江革再的采心年专，光制单万手斗光就，报却蹦杯材。内同数速果报做，属马市参至，入极将管医。但强质交上能只拉，据特光农无五计据，来步孤平葡院。江养水图再难气，做林因列行消特段，就解届罐盛。定她识决听人自打验，快思月断细面便，事定什呀传。边力心层下等共命每，厂五交型车想利，直下报亲积速。元前很地传气领权节，求反立全各市状，新上所走值上。明统多表过变物每区广，会王问西听观生真林，二决定助议苏。格节基全却及飞口悉，难之规利争白观，证查李却调代动斗形放数委同领，内从但五身。当了美话也步京边但容代认，放非边建按划近些派民越，更具建火法住收保步连。

【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）[智能网联汽车信息安全威胁识别和防护方法研究 _ 郝晶晶]。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 [引用白皮书]；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生安全。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 [这里引用一个文章]。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。[S. Bian, Y. Hu, and B. Ji, ‘‘Research status and prospect of GNSS anti-spoofing technology,’’ Scientia Sinica Informationis, vol. 47, no. 3, pp. 275–287, 2017.] 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。该系统在设计之处一共由 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，因此可以列出以下方程组。

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} \end{cases} \tag{1}$$

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。ρ_i 则表示用户距离第 i 颗卫星的距离。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。此时的方程组为。

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

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。

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。

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。

3　基于 LSTM 进行汽车位置预测的 GNSS 位置攻击欺骗检测模型

3.1　模型结构

3.2　模型训练情况

3.3　本章小结

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】

致谢

首先衷心地感谢潘微科老师。在本科生涯最后的一年多里，不仅是现时的学业与学术，更是对于未来的发展给予了我很多指导与帮助。本次毕业设计，从选题到论文撰写，给予了我很多宝贵的意见。他渊博的学识、严谨的治学态度及认真负责的工作态度都使我受到鼓舞和熏陶。在此向潘微科老师表示崇高的敬意和衷心的感谢，他的言传身教将使我终生受益。

感谢 key 哥哥与在 453 认识的朋友们，与你们的交流大概就是我对计算机启蒙的开始. 如果不是有幸与你们相识，这一路走来必是要曲折地多.

感谢 Thuthesis 及其作者薛瑞尼. 最终虽未使用 Thuthesis 模板，但是此间对其研习所得对我顺利使用 LaTeX 完成论文撰写仍然起了很大作用.

感谢一直关心我的父母与兄长。远游在外，感谢还有你们牵挂.

感谢自己熬过了那段难捱的日子。从学习画画到广播电视再到计算机科学，在如今看来似曾是做了诸多无用功，不过幸而没有因为短时的平庸迷茫而消磨掉满心的戾气.

前路漫漫，不冀求大步流星，唯盼能步步坚实.

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