车载导航 GPS 安全研究

陶 文 束 伟
扬州航盛科技有限公司，江苏 扬州 225009

[摘要]随着定位技术和汽车电子行业的发展，车载导航功能越来越完善，成为人们驾车出行的重要工具。车载导航最重要的基础是定位，主要方式是 GPS 卫星定位技术，然而传统的 GPS 定位存在信号抗干扰能力差的问题，导致 GPS 定位功能易收到外界信号攻击，导致无法正常定位。文中从信号干扰和信号欺骗角度分别进行了实际测试，选择的测试工具为 Hakcrf One，这是一款基于软件无线电技术的实验平台，通过 Gnu Radio Companion 软件实施信号干扰，通过 gps-sdr-sim 工具实现 gps 信号伪造，最终成功达到了预期目的。最后文中针对 gps 安全问题，提出了一些防护策略，可以有效提高 gps 安全性。
[关键词]车载导航；GPS；定位；安全；软件无线电
DOI：10.33142/sca.v6i6.9351 中图分类号：TP368.3 文献标识码：A

Research on GPS Safety for Vehicle Navigation

TAO Wen, SHU Wei
Yangzhou Hangsheng Technology Co., Ltd., Yangzhou, Jiangsu, 225009, China

Abstract: With the development of positioning technology and the automotive electronics industry, in car navigation functions are becoming more and more complete, becoming an important tool for people to travel while driving. The most important foundation of in car navigation is positioning, mainly through GPS satellite positioning technology. However, traditional GPS positioning has poor signal anti-interference ability, which makes GPS positioning functions susceptible to external signal attacks and unable to locate normally. In this paper, the actual tests are carried out from the perspective of signal interference and signal deception, and the selected test tool is Hakcrf One, which is an experimental platform based on Software-defined radio technology. Signal interference is implemented through Gnu Radio Companion software, and GPS signal forgery is achieved through GPS-SDR-SIM tool, and the expected purpose is finally achieved successfully. Finally, the article proposes some protective strategies to address the issue of GPS security, which can effectively improve GPS security.
Keywords: vehicle navigation; GPS; positioning; safety; software-defined radio

引言

车载导航作为汽车电子最重要的功能之一，为用户出行提供了重要帮助，正是因为其重要性，车载导航的安全问题需要引起产品开发人员的重视，尤其是 GPS 定位的安全问题是车载导航的重中之重，研究这个问题需要先了解 GPS 定位的基本原理，然后以实验方式论证其安全漏洞，最后针对已知的不足，提出改进措施。

1 背景介绍

1.1 GPS 定位系统组成

全球定位系统（Global Positioning System，简称 GPS）是一种由美国政府开发和维护的卫星导航系统，用于确定地球上任意位置的精确三维坐标。GPS 系统由一组空中和地面组件组成，它能够提供全球范围内的定位、导航和时钟同步服务。[1]

如下图所示为 GPS 系统的基本组成部分：

GPS 卫星：负责使用特定频率的信号广播轨道数据、时钟数据以及其他数据；

数据上传站：负责将地面站观测的卫星轨道数据发给指定的卫星；

主控制站：负责协调卫星、数据上传站、观察站；

用户终端：负责接收 GPS 信号，以便计算出用户的地理信息，比如经纬度、速度、方向等。用户终端通常具有内置的地图和导航功能，可以在屏幕上显示当前位置、导航路线和其他相关信息。

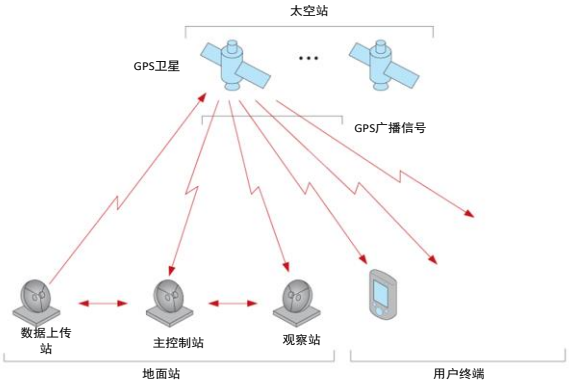

图 1 GPS 系统基本组成部分

1.2 GPS 卫星的工作原理

GPS 系统的核心部分是由 24 颗运行在中轨道的卫星

组成的卫星网络。这些卫星以高速绕地球运行，每天完成两次绕地球一圈的轨道。卫星之间通过无线电波进行通信，并向接收器传输精确的时间和位置数据。[2]

GPS 卫星的基本组成部分如下：

①太阳能电池板（Solar Panels）：GPS 卫星上配备了太阳能电池板，用于收集太阳能并将其转化为电能。这些电池板通常覆盖在卫星的表面，以提供卫星所需的电力。

②电源系统（Power System）：电源系统负责管理和分配电力以供给卫星的各个组件。它包括电池和电池充电回路，以便在卫星进入地球阴影时维持卫星的正常运行。

③通信系统（Communication System）：GPS 卫星上的通信系统用于与地面上的用户段和控制段进行通信。它包括天线、射频（Radio Frequency）发射器和接收器，用于发送和接收导航消息、定位数据和其他相关信息。

④控制系统（Control System）：控制系统用于管理卫星的姿态（姿态控制系统）和轨道（轨道控制系统）。它包括陀螺仪、加速度计和推进器等传感器和执行机构，以确保卫星保持在正确的轨道上并朝向目标方向。

⑤时钟系统（Clock System）：时钟系统是 GPS 卫星关键的组件之一，它提供高精度的时间信息。卫星上的原子钟通常用于提供精确的时间基准，以便用户端的接收器能够测量信号的传播时间并计算位置。

⑥导航载荷（Navigation Payload）：导航载荷负责存储和传输导航消息，包括卫星的身份、位置、时间和系统状态等信息。这些消息将被发送到用户端的接收器，以帮助计算位置和提供导航服务。

GPS 卫星的运行基本参数：

①轨道类型：GPS 卫星通常采用中地球轨道（Medium Earth Orbit，MEO）运行，这些卫星分布在大约 20，200 公里的高度上。

②轨道倾角：GPS 卫星的轨道倾角是指轨道与地球赤道面的夹角。GPS 卫星的轨道倾角通常接近 55 度，这种倾角可提供全球范围的覆盖。

③轨道周期：GPS 卫星的轨道周期是指卫星绕地球一周所需的时间。典型的 GPS 卫星轨道周期约为 12 小时。

④卫星数量：全球定位系统（GPS）系统至少包括 24 颗活跃卫星，这些卫星分布在不同的轨道上，以确保全球范围内的覆盖。

⑤发射频率：GPS 卫星发射导航消息和定位数据的频率通常为 1575.42 兆赫（MHz）。

⑥导航消息更新频率：GPS 卫星更新导航消息的频率通常为每秒一次。

⑦原子钟精度：GPS 卫星上的原子钟用于提供高精度的时间基准。这些原子钟的精度通常在纳秒级别，使 GPS 系统能够提供高精度的定位和导航服务。

1.3 GPS 定位原理

GPS 定位是指 GPS 接收器接收多颗卫星信号，解码数据，通过一定算法实现接收器位置的计算，大致过程如下图所示：

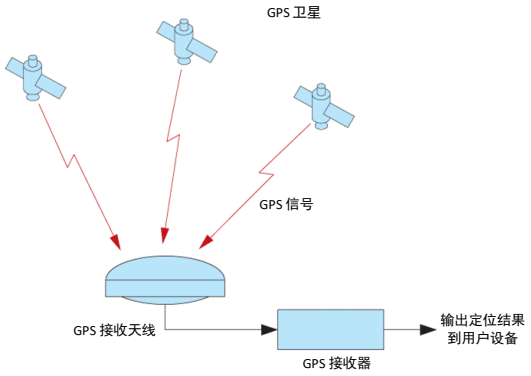

图 2 GPS 定位接收信号过程

①GPS 系统中的卫星定期发射导航信号，其中包含卫星的身份信息、位置信息和时间信息。

②GPS 接收器（安装在地面、车辆或设备上）通过天线接收到来自多颗卫星的信号。接收器测量接收到信号的传播时间。由于信号以光速传播，接收器可以通过测量传播时间来计算信号的传播距离。通过接收来自至少 4 颗不同卫星的信号，接收器可以进行多边测量。利用卫星的已知位置和测量的传播距离，接收器可以计算出自身的位置。

③GPS 接收器将计算出的位置信息或原始观测量数据输出到用户设备，比如手机、电脑、车载导航、工程测绘仪器等。

GPS 定位的基础是 Trilateration（三角测距）技术，它使用多个已知位置的点和到这些点的距离信息来确定未知点的位置。对于每个已知位置点，根据测量的距离，画一个以该点为圆心、距离为半径的圆。每个圆代表了与该基准点的距离固定的位置候选区域。通过观察这些圆的交点，即圆的交叉点或交点簇，可以确定未知点的位置。在理想情况下，三个定位基准点的交点将给出唯一的未知点位置。[3]如下图所示：

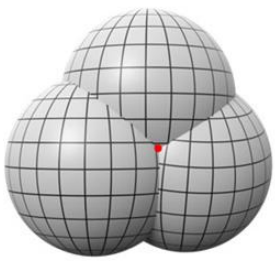

图 3 三角测距可以确定唯一点

Trilateration 方法要求至少 3 个已知位置点来进行定位，而 GPS 定位系统使用的是多边测量（Multilateration）方法，其中使用了至少 4 颗卫星来进行定位，这样可以解决卫星时间和接收器时间误差问题，从而提高定位精度和可靠性。示意图如下：

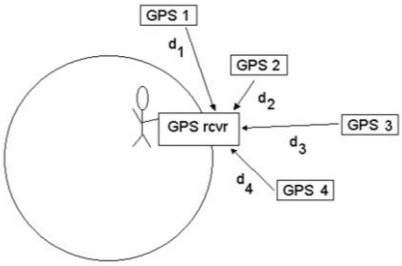

图 4　多边测量示意图

$$\begin{cases} d_1 = c(t_{t,1} - t_{r,1} + t_c) = \sqrt{(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2} \\ d_2 = c(t_{t,2} - t_{r,2} + t_c) = \sqrt{(x_2 - x)^2 + (y_2 - y)^2 + (z_2 - z)^2} \\ d_3 = c(t_{t,3} - t_{r,3} + t_c) = \sqrt{(x_3 - x)^2 + (y_3 - y)^2 + (z_3 - z)^2} \\ d_4 = c(t_{t,4} - t_{r,4} + t_c) = \sqrt{(x_4 - x)^2 + (y_4 - y)^2 + (z_4 - z)^2} \end{cases} \quad (1)$$

其中c为光速，$t_{t,i}$为第i颗卫星发出信号的时间，$t_{r,i}$为接收器接收到第i颗卫星信号的时间，t_c为卫星时钟和接收器时钟的时间偏差，x_i，y_i，z_i为第i颗卫星在$t_{t,i}$时间点的空间物理坐标，x,y,z为接收器的位置，即待求解未知数。

需要注意的是，以上只是理想情况下的模型，实际GPS定位精度受多种因素的影响。以下是一些主要的因素：

①卫星几何位置：GPS系统需要接收来自多颗卫星的信号才能进行定位。卫星的位置相对于接收器的分布和几何配置会影响定位的精度。较好的几何分布可以提高定位的精度。

②可见卫星数量：可见卫星的数量也会影响GPS定位的精度。更多的可见卫星意味着接收器可以获得更多的信号，并进行更精确的定位。

③天线质量：GPS接收器的天线质量也会对定位精度产生影响。高质量的天线能够更好地接收和处理卫星信号，从而提高定位的准确性。

④天线位置和遮挡物：天线的位置和周围的遮挡物也会影响GPS信号的接收质量。如果天线被高建筑物、树木或其他物体所遮挡，信号可能会受到干扰或削弱，从而影响定位的精度。

⑤大气条件：大气条件如天气状况、云层和大气湿度等也可能对GPS信号的传播产生影响。特别是在恶劣的天气条件下，如强烈的降水、雷暴等，信号的传播可能会受到干扰，导致定位精度下降。

⑥接收器质量：GPS接收器的质量和性能也会对定位精度产生影响。较高质量的接收器通常具有更好的信号处理和滤波功能，能够更准确地计算位置。

⑦信号多径效应：信号多径效应是指GPS信号在传播过程中遇到反射和散射，导致信号在接收器处产生多个到达路径，从而干扰原始信号。这可能会导致定位误差。

⑧时间同步误差：GPS定位是基于时间同步的原理，因此接收器和卫星之间的时间同步误差也会影响定位的准确性。

另外，GPS系统本身在设计上有一定的精度限制。在普通的民用应用中，通常可以达到数米至十米的定位精度。然而，在一些专业领域，如航空航天和测绘等，可能需要更高精度的GPS系统或采用其他补充技术来提高定位的精度。

1.4 车载导航工作原理

GPS定位在民用市场最重要的用途就是汽车电子导航，在电子导航普及之前，驾驶员跑长途需要通过纸质地图、问路等方式才能找到目的地。而有了电子导航，车主可以轻松的驾驶车辆沿着最优规划路线去任何有道路的地方，极大方便了人们驾车出行。

车载导航系统的基本结构如下所示：

图 5　车载导航基本构成

GPS接收器负责接收GPS卫星信号，并进行定位计算，输出原始数据（一般为NMEA0183格式）到SOC，由SOC的系统层（Linux或Android）进行解析，然后将导航需要的数据发给导航应用，导航应用通过定位引擎获取定位数据，基于地图资源数据，采用特定的路径规划算法生成规划路径，然后显示引擎会合成各信息图层，最终输出到车载屏幕上，为驾驶人提供导航帮助。[4]

1.5 GPS安全影响

由于GPS定位结果直接影响车载导航的效果，而车载导航的效果直接决定了汽车行驶安全，因此GPS的安全性至关重要，GPS系统安全主要分为以下几个方面：

①信号干扰：GPS信号可以受到人为干扰或自然干扰的影响。人为干扰可能包括恶意干扰设备（如GPS干扰器）的使用，以阻碍或扰乱GPS信号。自然干扰可能包括地理环境（如高建筑物、峡谷等）对信号的阻挡或多路径传播导致的信号衰减。这些干扰可能导致GPS接收器无法正确接收或解码信号，从而影响导航的准确性和可靠性。

②位置欺骗：GPS信号可以被伪造或篡改，导致接收器误读或接收到错误的位置信息。恶意用户可以使用GPS欺骗技术，通过发送虚假信号来欺骗接收器，使其显示错误的位置或导航信息。这可能导致驾驶员误解当前位置、错误的导航决策，或者被导向危险的区域。[5]

③安全漏洞：GPS系统本身可能存在安全漏洞，可能会被黑客利用进行攻击。例如，恶意用户可能通过操纵GPS信号或利用GPS接收器的漏洞来获取未经授权的访问或控制权，从而对导航系统、车辆或用户信息造成威胁。

2 GPS安全攻击测试

本文通过实践的方法对GPS的安全问题进行研究，主要进行了信号干扰测试、信号回放攻击测试和信号欺骗测试，评估各项测试对实际车载导航产品的影响。

测试使用了SDR（Software Defined Radio软件无线电）的方法产生干扰信号，SDR是一种无线通信技术，通

过软件来实现无线电信号的处理和调制，而不需要硬件电路的改变。传统的无线电系统通常使用硬件电路来执行信号处理功能，如滤波、调制和解调等。而 SDR 则使用可编程的数字信号处理器（DSP）和通用计算机来实现这些功能。[6]

市场上常用的 SDR 工具是 Hackrf One， 由 Michael Ossmann 及其公司 Great Scott Gadgets 开发，是一款功能强大、灵活可定制的开源 SDR 平台，它覆盖了 1 MHz 至 6 GHz 的频率范围，可应用于多个领域，如无线通信研究、无线电频谱分析、无线电信号重放、无线电侦听等等。[7]

2.1 信号干扰测试

测试目的：

通过同频 GPS 信号干扰方式，影响 GPS 接收器接收卫星信号，从而使得车载导航无法定位。

测试思路：

GPS 常用频段为 L1 频段，其中心频点为 1575.42 MHz，即载波频率，GPS 信号常用的调制方式为 BPSK（载波相移键控），它使用两个相位状态（0 度和 180 度）来表示数字位，通常用于传输导航数据。在 BPSK 调制中，0 和 1 被映射到正弦波载波的相位变化。如果输入数据是 0，则相位不变；如果输入数据是 1，则相位反转 180 度。

测试环境：车载导航主机一台、Hackrf One 一台、PC 一台，如下所示：

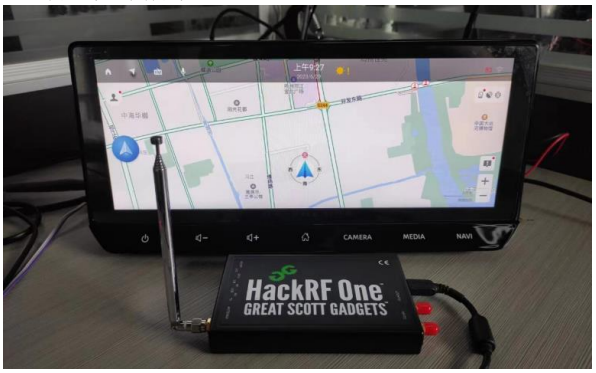

图 6 实际测试环境

测试方式：

使用 GNU Radio Companion 软件输入随机数据，按照 BPSK 调制到 GPS L1 频点上（1575.42 MHz），然后通过 Hackrf One 将射频信号发射出去，评估对车载导航定位的影响程度，如下是 GNU Radio Companion 数据流图：

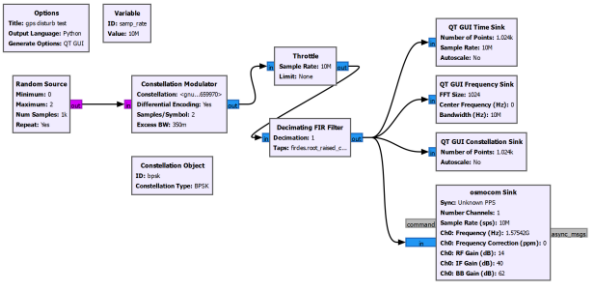

图 7 GPS 干扰测试流程图

测试结果：

发射 BPSK 干扰信号之前，1575.42 MHz 频段频谱噪声小，车载导航搜星、定位均正常：

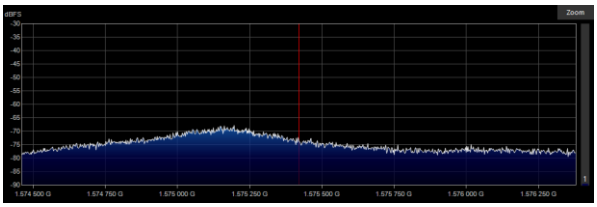

图 8 正常环境下 GPS L1 频谱干扰小

图 9 导航搜星、定位正常

发射干扰 BPSK 信号后，GPS L1 频谱几乎被高功率噪声淹没，如下所示：

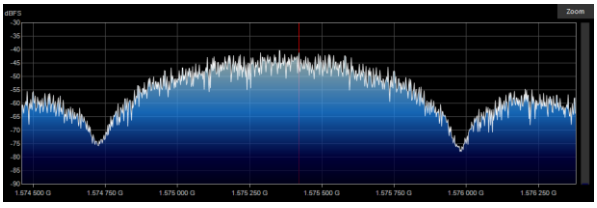

图 10 发射干扰信号后的 GPS 频谱

同时车载导航无法正常定位、几乎完全搜不到 GPS 卫星，如下所示：

图 11 发射干扰信号后导航无法定位

小结：通过将随机噪声按 BPSK 调制后，用 Hackrf One 在 GPS L1 频段上发射射频信号，可以明显压制正常 GPS 信号，导致车载导航无法获取卫星数据，造成定位失败。

2.2 信号欺骗测试

测试目的：

使用 Hackrf One 发射伪造的 GPS 信号给车机，使得

车载导航定位到错误的位置。[8]

测试方法：

①首先在 google earth 中任意选择一个目的地，我们选择上海东方明珠电视塔，经纬度为：北纬 31.241102°，东经 121.495616°，在地图中的位置如下所示：

图 12 google earth 中的目标点

②然后使用 gps-sdr-sim 生成该目标位置的模拟 GPS 信号数据：

./gps-sdr-sim -e brdc1800.23n -l 31.241102，121.495616，10 -b 8

执行后会生成 gpssim.bin 文件。

③最后使用 Hackrf One 设置合适的参数发射该 bin 文件：

hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 40

测试结果：发射伪造 GPS 数据前，车载导航定位位置为作者所在位置，如下蓝色箭头所示：

图 13 车载导航定位到正确位置

发射伪造 GPS 数据后，等待几分钟，车载导航会重新定位到上海东方明珠预设位置，如下图所示：

图 14 车载导航定位到假位置

小结：通过 SDR 方式发射伪造 GPS 信号可以造成车载导航定位到错误的位置。

3 GPS 安全防护策略

车载导航 GPS 的安全性非常重要，它直接关系到驾驶安全和乘车体验。但是由于 GPS 定位对卫星信号非常依赖，而卫星信号本身缺乏有效的加密和抗干扰能力，导致 GPS 接收器很容易收到外界干扰，导致定位失败。因此如何提高车载导航定位的安全性迫在眉睫，如下是一些可行措施：[9]

3.1 基于 GNSS 定位的防护策略

GNSS（全球导航卫星系统）是一种利用多颗卫星提供全球定位和导航服务的技术。GNSS 系统包括多个卫星系统，其中最知名的是美国的 GPS（全球定位系统），还有俄罗斯的 GLONASS、欧盟的 Galileo、中国的北斗导航系统等。

传统的GPS定位通常使用3颗以上的卫星信号来进行三角定位，计算出接收器的位置。而 GNSS 多星定位则利用更多的卫星信号，可以提高定位的准确性、可靠性和鲁棒性。

通过使用多颗卫星的信号，GNSS 多星定位可以克服单一卫星信号受到阻塞、遮挡或干扰的问题。当一颗卫星的信号不可用时，仍然可以通过其他卫星的信号进行定位。这种冗余性可以提高系统的可靠性，特别是在复杂的环境中，如城市峡谷、森林、高楼大厦等。

此外，GNSS 多星定位还可以提供更精确的定位结果。通过使用更多的卫星信号，可以进行更精确的三角定位计算，减少误差和不确定性。这对于需要高精度定位的应用领域（如精密测量、航空导航、精密农业等）尤为重要。

3.2 基于 GPS 多频定位的防护策略

GPS 多频定位是一种利用多个频率的 GPS 信号进行位置计算的技术。传统的 GPS 接收器通常只接收 L1 频率的信号进行定位，但现代的 GPS 接收器可以同时接收 L1、L2 和 L5 等多个频率的信号。

使用多频信号进行定位可以提供以下几个优势：

①抗多路径干扰：多路径干扰是 GPS 信号在传播过程中反射、折射等现象导致的信号多次到达接收器的问题。通过接收多个频率的信号，可以对多路径干扰进行更好地抑制和分离，提高定位的准确性和可靠性。

②抗多频干扰：在一些恶意干扰或无意干扰的情况下，可能会有特定频率的信号被干扰或屏蔽。通过使用多频信号，接收器可以在受到特定频率干扰时，仍然能够利用其他频率的信号进行定位，减少干扰对定位结果的影响。

③提高精度和可靠性：不同频率的 GPS 信号在传播过程中受到大气和离子层等因素的影响程度不同。通过同时接收多个频率的信号，可以校正这些影响，提高定位的精度和可靠性。特别是接收 L2 和 L5 频率信号可以提供更准确的定位结果。

③提高完整性和鲁棒性：多频定位可以提供更多的冗余信息，从而增加系统的完整性和鲁棒性。当某个频率的信号受到干扰或故障时，其他频率的信号可以提供备用的信息，确保定位系统的可靠性和稳定性。

综上所示，GPS 多频定位利用多个频率的信号进行位置计算，具有抗干扰、提高精度和可靠性的优势。

3.3 基于多种定位方法的防护策略

车载导航除了卫星定位，还可以借助其他辅助定位手段提高定位的安全和可靠性，如下是一些可用的定位方案：

①INS（惯性导航系统）：惯性导航系统由加速度计和陀螺仪等惯性传感器组成。加速度计测量车辆在三个轴向上的加速度，而陀螺仪测量车辆围绕三个轴向的角速度。通过对这些测量值进行积分，可以得到车辆的速度、位移和方向变化。INS 导航在车载导航系统中通常作为辅助定位方法与其他定位技术（如 GPS）结合使用，以提供更准确和可靠的车辆定位。

②基站定位：车载导航系统可以利用 GSM、LTE 网络基站的信号来进行定位。通过测量与多个基站之间的信号强度和时延差异，可以估计车辆的位置。

③Wi-Fi 定位：这是一种基于无线局域网（Wi-Fi）信号的定位方法，通过测量车辆周围可用 Wi-Fi 网络的信号强度和位置信息来推断车辆的位置。当车辆处于 Wi-Fi 信号范围内时，车载导航系统可以扫描周围的 Wi-Fi 信号，并将其与预先存储的 Wi-Fi 数据库进行匹配。通过比对信号强度和位置信息，系统可以推断车辆当前的位置。

④车辆辅助系统（V2V、V2X）：一些现代车辆配备了车辆间通信系统，可以与周围车辆进行通信，并通过交换位置和运动信息来实现相对定位。

综上，采用多种定位融合的方法可以避免单一定位系统被攻击，从而有效提高了车载导航定位的可靠性和安全性。

4 结束语

车载导航可以准确获取当前汽车位置，并进行路径规划，引导用户准确到达目的地，极大提升了用户的出行体验。而 GPS 定位作为车载导航的基础，发挥了重要的作用，然而 GPS 定位依赖卫星信号接收，因此本身存在一些安全风险，本文从信号干扰和信号欺骗的角度，分别模拟了攻击手段，经研究和调试，达到了预期的实验目的，证明了 GPS 定位的脆弱性。基于此原因，本文进一步提供了一些改善 GPS 定位可靠性差的方法和策略，希望未来用户驾车出行可以更方便、更准确、更安全。

[参考文献]

[1]刘艳荣.GPS 定位原理及其在工程测量中的应用[J].中文科技期刊数据库(全文版)工程技术,2016(5):206.
[2]范伟,王贵文,刘发发.GPS 卫星轨道位置计算方法的研究[J].山西师范大学学报,2015(4):63-68.
[3]王红力,张光明.GPS 定位技术与误差[J].中国科技信息,2010(6):85-87.
[4]施文灶,王平.GPS 车载导航系统的设计[J].软件,2014(4):32-36.
[5]廖琪,郝金明,郑娜娥,等.基于轨迹欺骗的 GPS 导航干扰试验研究[J].信息工程大学学报,2022(2):141-145.
[6]都汉场.软件无线电技术的发展应用探究[J].科技创新与应用,2015(24):54-55.
[7]田兆丰,文勇军.基于 HackRF 的软件无线电扩展应用研究[J].信息与电脑,2018(7):24-25.
[8]王鹏,郝小龙,朱耀康,等.防止恶意无人机入侵电力巡检区的管控方法[J].网络与信息安全学报,2018,4(6):70-76.
[9]李馥娟,王群.GPS 欺骗攻击检测与防御方法研究[J].警察技术,2018(1):45-48.

作者简介：陶文（1985.11—），男，江苏扬州人，汉族，硕士，工程师，主要从事汽车子嵌入式软件开发；束伟（1983.8—），男，江苏扬州人，汉族，硕士，工程师，主要从事汽车子嵌入式软件开发。