

基于广播通信信道的轻量级车辆轨迹安全验证方案

宁志强¹, 汪媛媛¹, 张驰¹, 魏凌波¹, 俞能海¹, HAO Yue²

(1. 中国科学技术大学网络空间安全学院, 安徽 合肥 230001;

2. San Francisco State University, Department of Computer Science, Houghton, San Francisco, CA 94132)

摘要: 在智慧交通系统中, 智能汽车需要实时广播车辆轨迹消息来协调驾驶决策, 保证行车安全。然而, 攻击者可以通过修改消息的发送时间戳或操纵信号发射的载波频率伪造车辆轨迹。针对该问题, 提出了一种轻量级车辆轨迹验证方案。无须任何特殊硬件支持, 基于同一广播通信信道完成对车辆轨迹的安全验证; 无须时间同步, 每个验证点计算消息接收时间与发送时间戳的时间间隔, 通过联立两两验证点的时间间隔所形成的空间位置约束方程, 达到了抗时间戳伪造攻击的防御效果; 每个验证点计算消息到达频率和预定发射频率的多普勒频移, 通过联立两两验证点的频移所形成的速度矢量约束方程, 实现了抗载波频率操纵攻击的安全目的。通过形式化分析, 表明增加验证点的数目可以提高车辆轨迹验证的准确率。最后, 真实环境中的实验结果表明, 当验证点数量设定为3个时, 方案展现出了最佳的性能。与现有方案相比, 在分别验证真实车辆轨迹和虚假车辆轨迹时, 方案具有更高的正确率, 更低的错误拒绝率和错误接受率。

关键词: 时间戳; 多普勒效应; 车辆轨迹; 安全验证

中图分类号: TP302

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023077

Lightweight and secure vehicle track verification scheme via broadcast communication channels

NING Zhiqiang¹, WANG Yuanyuan¹, ZHANG Chi¹, WEI Lingbo¹, YU Nenghai¹, HAO Yue²

1. School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230001, China

2. Department of Computer Science, San Francisco State University, San Francisco, CA 94132, USA

Abstract: In intelligent transportation systems, it is crucial for smart vehicles to broadcast real-time vehicle track messages to coordinate driving decisions and ensure driving safety. However, attackers can manipulate vehicle tracks by modifying timestamps or manipulating signal frequencies, posing a threat to security. To address this problem, a lightweight vehicle track verification scheme was proposed, utilizing the broadcast communication channels to achieve secure verification of vehicle tracks without any special hardware support. Without time

收稿日期: 2023-03-21; 修回日期: 2023-08-18

通信作者: 张驰, chizhang@ustc.edu.cn

基金项目: 国家自然科学基金 (61871362, U19B2023)

Foundation Item: The National Natural Science Foundation of China(61871362, U19B2023)

引用格式: 宁志强, 汪媛媛, 张驰, 等. 基于广播通信信道的轻量级车辆轨迹安全验证方案[J]. 网络与信息安全学报, 2023, 9(5): 71-81.

Citation Format: NING Z Q, WANG Y Y, ZHANG C, et al. Lightweight and secure vehicle track verification scheme via broadcast communication channels[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 71-81.

synchronization, each verifier calculated the time interval between the reception time of the message and the sending timestamp. Spatial position constraint equations are formulated by combining these time intervals between any two verifiers, effectively defending against timestamp forgery attacks. Additionally, each verifier calculates the Doppler frequency shift between the arrival frequency and the scheduled transmit frequency. Velocity vector constraint equations were formulated by combining these frequency shifts between any two verifiers, providing defense against carrier frequency manipulation attacks. Formal analysis shows that increasing the number of verifiers improves the accuracy of the proposed verification scheme. Experimental results in a real-world environment further validate that the proposed verification scheme exhibits the best performance when the number of verifiers is set to 3. Compared to the existing solution, the proposed verification scheme has a higher accuracy, lower false rejection rate, and lower false acceptance rate when validating true vehicle track and false vehicle track separately.

Keywords: timestamp, Doppler effect, vehicle track, secure verification

0 引言

随着汽车工业技术的迅速发展,智能汽车已经成为智慧交通系统的重要组成部分,给人们出行带来了极大便利。为了避免交通事故,智能汽车通常会安装摄像头、激光雷达、毫米波雷达等设备,探测并定位周围的汽车,并采取制动或避让等措施。然而,这种主动式的探测方法开销大,需要额外的设备成本和设备维护费用,同时,面临雨雪天气干扰、识别精度不高问题。此外,这种方法需要占用海量的车载计算资源进行数据实时处理,并且在探测范围上存在盲区,无法完全保障智能汽车在道路上的安全行驶^[1]。

在这样的场景下,被探测的智能汽车通常安装卫星定位系统(如北斗、GPS)、惯性测量单元、陀螺仪等传感器,以实现高精度定位,并通过广播通信信道向周围智能汽车或路边基础设施发送车辆轨迹信息^[2],如车辆位置、速度、加速度等。周围的智能汽车或路边基础设施通过侦听广播通信信道的方式获取信息^[3],进而根据被探测智能汽车的车辆轨迹下达行车指令,改变行车速度和方向。这种被动式广播车辆轨迹信息的方式仅依赖于现有的车载传感器和通信模块,并未增加任何特殊硬件^[4]。该方式的优点在于它降低了开销,同时减少了对车载计算资源的需求。此外,该方式有利于高速公路车辆编队行驶,可以更好地保持合适的行驶速度和车间距离,实现轻量级的车辆定位应用^[5]。然而,这种方式也存在安全隐患:一方面,如果车载传感器发生故障并输出错误轨迹数据,这些错误数据会被广播到

周围的智能汽车,导致这些汽车做出错误的决策,如如果需要减速的车辆根据错误轨迹数据加速行驶,将会导致严重的交通事故^[6];另一方面,恶意的攻击者在通过控制车载软件平台后,可以伪造虚假的车辆轨迹信息并发送给周围的智能汽车,如果这些汽车没有任何安全防御机制,就会根据虚假的车辆轨迹下达错误的行车指令,导致出现严重的后果^[7]。因此,对智能汽车广播的车辆轨迹信息进行安全验证是非常必要的^[8]。

现有的车辆轨迹安全验证方法研究可以总结为两种:第一种方法通常在智能汽车上部署硬件,如通过车载激光雷达等设备进行主动探测,或通过增加特殊硬件的方法对接收到的车辆广播信号进行物理特征提取,从而定位车辆位置;第二种方法在不部署任何特殊硬件的情况下,利用通信信道获取车辆状态信息,验证车辆轨迹。Yan 等^[9]提出一种基于车载雷达的方法,通过探测邻近车辆并计算雷达数据与邻近车辆广播数据之间的余弦相似度来判断广播数据是否真实;从过滤后的真实数据中筛选出虚假数据,实现对邻近车辆轨迹的验证。然而,该方案开销较大,同时需要多个不同节点的车载雷达实现安全防御。Sun 等^[5]利用单个天线接收器测量信号到达角(AoA, angle of arrival)和到达频率(FoA, frequency of arrival),定位发射信号的车辆。该方案利用环境中的多路径信号反射点来模拟不同位置的验证点,并使用极大似然估计模型定位可能的信号源,同时基于到达频率差的方法消除未知频率偏移,并利用多普勒效应验证车辆速度。然而,当车辆在开阔的道路环境行驶时,由于不存在反射物体,

车辆接收不到反射信号。Du 等^[10]设计了一种名为 MobTrack 的单设备系统, 该系统增加多根天线, 利用天线阵列计算视距 (LoS, line of sight) 传播信号的到达角来测量信号源的位置, 实现轨迹验证。然而, 智能汽车搭载的硬件有时会发生故障^[11], 这可能会产生错误的信息。

如果不部署任何特殊硬件, 仅基于广播通信信道来获取车辆状态信息, 也可以对车辆轨迹进行验证。通常采用测距的方法来解决此问题^[12]。Baker 等^[13]提出一种通过测量信号从固定节点传输到移动节点时的到达时间差来实现对固定节点位置安全验证的方法。然而, 该方法在一定误差范围内有效, 并且需要各个节点保持精确的时间同步。Yao^[14]等提出了 Voiceprint 方法, 通过观察接收信号强度指示 (RSSI, received signal strength indicator) 在两个节点上的时间序列是否相似来实现对节点位置的验证, 而无须依赖任何无线电传播模型。然而, 恶意攻击者可以改变本地时间, 这会使消息接收方无法验证两个节点是否保持精确的时间同步。

基于对广播通信信道频偏的测量也可以对智能汽车的速度进行验证。Sun 等^[15]提出在后方车辆获得前方目标车辆广播的消息后, 基于后方车辆与另一台可信车辆测量信号到达角以及相应的信号到达频率差, 通过卡方检验检测这些数据, 从而验证目标车辆轨迹。然而, 恶意攻击者可以通过调整智能汽车载波信号的频率进行欺骗, 周围车辆不能根据信号的到达频率验证目标车辆的速度。

针对上述问题, 本文提出了一种基于广播通信信道的抗时间戳伪造攻击和抗载波频率操纵攻击的轻量级车辆轨迹安全验证方案, 本文的主要贡献如下。

1) 提出了一种基于广播通信信道的轻量级车辆轨迹安全验证方案。该方案无须部署任何特殊硬件, 基于同一广播通信信道, 完成对车辆轨迹的安全验证。

2) 提出了一种抗时间戳伪造攻击的车辆轨迹安全验证方法。该方法计算每个验证点计算消息接收时间与发送时间戳的时间间隔, 通过联立两两验证点的时间间隔所形成的空间位置约束方

程, 达到抗时间戳伪造攻击的防御效果。

3) 提出一种抗载波频率操纵攻击的车辆轨迹安全验证方法, 利用多普勒效应验证智能汽车的瞬时速度, 每个验证点计算消息到达频率和预定发射频率的频偏, 通过联立两两验证点的频偏所形成的速度矢量约束方程, 实现抗载波频率操纵攻击的安全目的。

4) 真实环境的实验结果表明, 当存在至少 3 个验证点时, 可以对车辆的轨迹进行安全验证, 并达到抗时间戳伪造攻击和抗载波频率操纵攻击的效果。

1 模型假设

1.1 系统模型

车辆轨迹安全验证的场景通常包含目标车辆、验证者、验证点等。目标车辆不断广播自身的轨迹信息, 并通过消息验证码或数字签名的方式确保广播的信息未被修改。验证者需要验证这些广播信息内容的真实性。验证点是位于智能汽车的广播范围内, 能够接收到智能汽车发送的物理层无线通信信号, 起到辅助验证者验证车辆轨迹作用的实体。这类实体有两类: 第一类是路侧单元和基础设施; 第二类是周边车辆。路侧单元和基础设施具有较强的安全防护能力, 在充当验证点时可认为是可信的。周边车辆能够接收到目标车辆广播的消息, 也可以充当验证点的作用, 然而需要验证者信任这些周边车辆, 这可以通过信誉机制^[16]予以解决。验证者可以接收来自各个验证点有关目标车辆的轨迹验证信息, 然后在本地综合判断目标车辆广播信息的可信度。因此, 验证者无须位于智能汽车广播范围内。为了简化讨论, 后续描述中假设验证者就是某一可信的验证点。

本文假设所有验证点可以与验证者安全地通信, 并且所有验证点可以正确地将自身位置发送给验证者。由于在验证过程中, 验证点都是可信的, 验证点直接将目标车辆的消息发送给验证者, 验证点与验证者之间的安全通信将保证所有消息都真实地来自目标车辆。所有验证点可以正确地将自身位置发送给验证者, 使得验证者可以根据验证点的位置验证目标车辆的真实位置。

本文假设验证点可以记录接收车辆消息时的本地时间，并将车辆消息和到达的本地时间、车辆消息的到达频率等信息传输给验证者。在此过程中，由于验证者与验证点的距离不影响本文的验证方案，验证点传输信息给验证者的时间可以忽略不计。

本文假设目标车辆与验证点之间不需要严格的时间同步，为了实现此目标，需要将时间分为本地时间和全局时间，本地时间表示以本地物理时钟为时间基准的时间，本地时间戳表示以本地时间为时间基准标记的时间戳，全局时间表示在各个物理时钟存在偏移的情况下，以此时间作为参考的标准时间。

本文假设智能汽车定期使用固定信号频率向周围广播消息，该消息包括自身的位置、速度、发送消息时车辆的本地时间戳等。定期广播消息是为了让周围验证点可以稳定地接收车辆消息，以便安全验证车辆轨迹。使用固定信号频率可以使所有验证点统一地在同一个信号频率上接收目标车辆的消息，并且验证点可以根据信号的到达频率差对车辆的速度进行验证。

目标车辆以一个固定信号频率 f_1 连续广播车辆消息，所有位于目标车辆通信范围内的验证点都可以接收到车辆消息。本文用 O 表示固定的验证点， $S = \{M_1, \dots, M_k\}$ 表示车辆轨迹消息集合， $|S| > 1$ ，对于目标车辆广播的两条车辆消息 $M_i = (\vec{v}_i, p_i, t_i)$ 和 $M_{i+1} = (\vec{v}_{i+1}, p_{i+1}, t_{i+1})$ ， $p_i \neq p_{i+1}$ ， t_i 表示车辆消息 M_i 发送时的本地时间戳， p_i 表示在时间节点 t_i 时的车辆位置（二维或三维的欧几里得坐标）。从消息 M_i 的定义可以得知目标车辆在时间节点 t_i 向周围车辆广播其本地消息时间戳、位置和速度， $\vec{v}_i$ 表示在位置 p_i 时的车辆速度。

目标车辆消息显示的车辆轨迹如图 1 所示，从目标车辆发送给验证点 O_a 的车辆消息显示其位置从 p_1 依次移动至 p_2 、 p_3 。目标车辆使用无线通信信道先后将车辆消息 M_i 和 M_{i+1} 广播到验证点 O_a ，验证点的位置位于 p_a 。以验证点 O_a 为例，本文规定 $\vec{v}_i^a$ 表示车辆消息沿着验证点 O_a 的径向速度， θ_i^a 是车辆速度 $\vec{v}_i$ 与目标车辆到验证点视线路径的角度， v_i 和 v_i^a 是车辆速度 $\vec{v}_i$ 和径向速

度 $\vec{v}_i^a$ 的标量大小， v_i^a 和 v_i 关系式为

$$v_i^a = \cos(\theta_i^a) \cdot v_i$$

在多普勒效应的影响下，验证点 O_a 可以接收到沿着径向速度方向的车辆消息，其中 v_c 表示信号的传播速度，验证点 O_a 接收到目标车辆消息的预期信号频率 f_a 为

$$f_a = \frac{f_1}{1 - v_i^a / v_c} \quad (1)$$

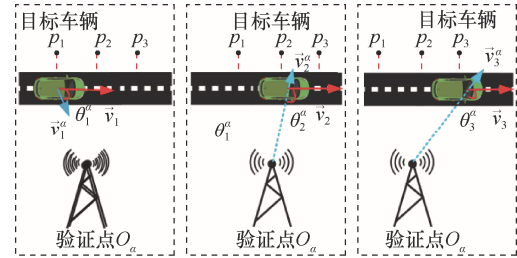


图 1 目标车辆消息显示的车辆轨迹
Figure 1 Track information broadcasted by the target vehicle

本文所要实现的安全目标是验证目标车辆先后发送给验证点的车辆消息 M_i 和 M_{i+1} 是否真实。

1.2 攻击模型和假设

为了分析所提车辆轨迹安全验证方案，本文使用以下威胁模型。假设在位置 p_A 有一攻击者 A ，可以是恶意车辆，也可以是软件平台被攻击者控制的车辆。该攻击者的主要目的是广播被虚假的车辆消息欺骗的位于自身通信范围内的验证点。

虽然在攻击者的通信范围内存在众多验证点，然而并非所有的验证点都参与对车辆消息的安全验证过程，因而攻击者无法确认在验证过程中参与的验证点的具体位置和数量，无法采用定向天线进行欺骗攻击，或者攻击者控制了车辆的软件平台，但无法改变车辆的通信硬件，因此只能采用全向天线广播车辆消息，这使得验证点都能够通过广播信道接收到相同的车辆消息。

攻击者可以修改车辆位置 p_i 和车辆消息时间戳 t_i ，完成时间戳伪造攻击；修改车辆位置 p_i 、预定的广播信号频率 f_1 、标量速度 v_i ，完成载波频率操纵攻击。首先，攻击者与验证点各自的本地物理时钟可以不同步，消息时间戳 t_i 不一定与

全局时间相同，这使攻击者可以进行消息时间戳的伪造攻击，即攻击者可以在本地对消息时间戳进行任意篡改，使消息的发送时间戳与本地的物理时间不对应，进而可以在任意时间节点上广播任意位置，而验证点无法对单个消息中的时间戳进行验证^[13]。其次，验证点不具备任何特殊硬件对目标车辆的位置和速度进行测量，因而攻击者可以任意篡改 p_i 和 $\vec{v}_i$ 。攻击者还可以选择不同的载波频率 f_A 发射信号，即控制信号载波频率 f_i 对验证点进行欺骗攻击，使验证点无法根据信号的到达频率差对车辆消息内容的 $\vec{v}_i$ 进行验证^[17]。

2 本文方案设计

本文方案通过对消息时间戳的计算和基于多普勒效应的应用，实现对车辆轨迹的安全验证。方案分为两部分：消息时间戳的验证方法和信号载波频率的验证方法。

2.1 消息时间戳的验证方法

由于目标车辆与验证点各自的物理时钟存在偏差，为了便于讨论，本文将时间区分为全局时间和本地时间。全局时间用 T 表示，在全局时间中两个时间节点之间的时间间隔用 D 表示；本地时间用 t 表示，在本地时间中两个时间节点之间的时间间隔用 d 表示。

图2展示了目标车辆与验证点间车辆消息传输的全局时间线。从全局时间角度来说，车辆消息 M_i 从目标车辆位置到达验证点位置的传播时延为 $D_i^a = T_i^a - T_i$ ，其中 T_i 表示目标车辆发送车辆消息 M_i 的时间点， T_i^a 表示验证点 O_a 接收到车辆消息时的时间点。目标车辆发送消息 M_i 和 M_{i+1} 间的时间间隔表示为 $D_{i,i+1} = T_{i+1} - T_i$ 。验证点 O_a 接收到 M_i 和 M_{i+1} 之间的时间间隔表示为 $D_{i,i+1}^a = T_{i+1}^a - T_i^a$ 。从本地时间角度来说，若目标车辆发送的两次车辆消息 M_i 和 M_{i+1} 是真实的，则有 $d_{i,i+1} = D_{i,i+1}$ 。

基于以上定义，车辆轨迹安全验证流程如下。由图2可知，目标车辆发送消息 M_i 到验证点 O_a 接收消息 M_{i+1} 的时间间隔 $D_{i,i+1}^a + D_i^a$ 应等于消息 M_i 和消息 M_{i+1} 的发送时间间隔 $D_{i,i+1}$ 与消息 M_{i+1}

的传播时延 D_{i+1}^a 之和，即

$$D_{i,i+1}^a + D_i^a = D_{i,i+1} + D_{i+1}^a \quad (2)$$

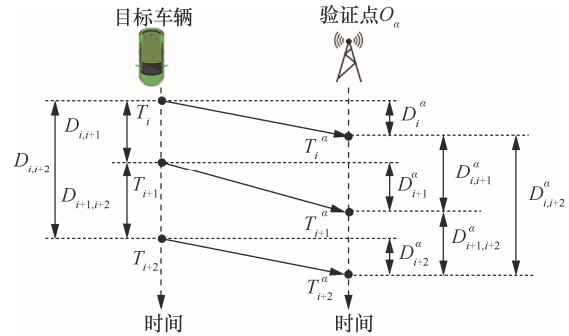


图2 目标车辆与验证点间车辆消息传输的全局时间线
Figure 2 The message transmission between the target vehicle and the verifier with a global timestamp

从全局时间角度来说，车辆消息 M_i 和 M_{i+1} 被发送到验证点 O_a 位置的传播时延可以分别表示为 $D_i^a = \|p_i - p_a\|/v_c$ ， $D_{i+1}^a = \|p_{i+1} - p_a\|/v_c$ ，其中 v_c 表示信号传播速度， $\|\cdot\|$ 代表欧几里得距离。

由式(2)可知，验证点接收消息 M_i 和 M_{i+1} 的时间间隔 $D_{i,i+1}^a$ 为

$$D_{i,i+1}^a = D_{i,i+1} + (D_{i+1}^a - D_i^a) \quad (3)$$

从本地时间角度来说，验证点 O_a 接收 M_i 和 M_{i+1} 间的时间间隔表示为 $d_{i,i+1}^a$ 。验证车辆轨迹是否真实的关键在于：从本地时间来看，验证点 O_a 接收消息 M_i 和 M_{i+1} 间的时间间隔 $d_{i,i+1}^a$ ，是否等于目标车辆发送消息 M_i 到验证点接收消息 M_{i+1} 间的时间间隔与消息 M_i 的传播时延 D_i^a 之差；无论用全局时间还是本地时间，目标车辆发送 M_i 和 M_{i+1} 的时间间隔始终相同，即 $D_{i,i+1} = d_{i,i+1}$ 。对于任意车辆消息 $M_i, M_{i+1} \in S$ ，每个验证点都需要判断是否满足下列条件。

$$d_{i,i+1}^a = d_{i,i+1} + (D_{i+1}^a - D_i^a) \quad (4)$$

由于时间测量误差等因素存在，测量得到的 $d_{i,i+1}^a$ 与真实数值不完全相同，因而当绝对误差小于阈值 τ_1 时，即 $|d_{i,i+1}^a - (d_{i,i+1} + D_{i+1}^a - D_i^a)| \leq \tau_1$ ，可认定消息 M_i 和消息 M_{i+1} 都是真实可信的。

2.2 信号载波频率的验证方法

由多普勒效应可知^[5]，传输信号频率大小与距离无关，与速度有关。不同方向上的径向速度

不相同,所有验证点接收到的信号载波频率也不相同。每个验证点由式(1)计算出预期信号频率,如果每个验证点接收到的信号载波频率与计算出的预期信号频率不相同,就会引发警报。以验证点 O_α 为例, f_α 是验证点 O_α 接收到的信号载波频率, f_1 是车辆固定发出的载波信号频率, v_i^a 是载波信号沿着验证点 O_α 的径向速度大小, v_c 表示信号的传播速度,对于车辆消息 M_i ,每个验证点 O_α 都需要判断是否满足下列条件。

$$f_{\alpha} = \frac{f_1}{1 - v_i^{\alpha} / v_c} \quad (5)$$

由于信道噪声等因素存在,测量的 f_α 与真实的载波信号频率不完全相同,因而当绝对误差小于阈值 τ_2 时,即 $\left|f_\alpha - \frac{f_1}{1 - v_i^\alpha/v_c}\right| \leq \tau_2$,可认定消息 M_i 是真实可信的。

此外,在对车辆消息的载波信号进行验证时,各个验证点之间无须保持严格的时间同步,验证点与智能汽车也无须保持时间同步,这解决了各节点本地物理时钟不同步的问题。本文方案无须在智能汽车与验证点上部署特殊的硬件,这使得本文方案可以大规模、低成本地运用在车辆轨迹的安全验证上。而且本文方案可以在高速公路上快速验证智能汽车的瞬时速度,从而安全验证车辆轨迹。

3 安全性分析

3.1 基于单个验证点的安全性分析

(1) 抗时间戳伪造攻击的安全性分析

假设目标车辆（或攻击者）会先后发送两次车辆消息 $M_i = (t_i, p_i)$ 和 $M_{i+1} = (t_{i+1}, p_{i+1})$ 给验证点 O_α ，且 $p_i \neq p_{i+1}$ 。对于任意两个车辆消息 M_i 和 M_{i+1} ，如果这些车辆消息被验证是安全的，即可证明车辆轨迹 $S = \{M_1, \dots, M_k\}$ 也是安全的。

当验证点数量为 1 时,从本地时间角度来说,由式(4)可知

$$t_{i+1}^\alpha - t_i^\alpha = (t_{i+1} - t_i) + (D_{i+1}^\alpha - D_i^\alpha) \quad (6)$$

攻击者目标是寻找消息发送时间点 T_i 和 T_{i+1} , 在 M_i 发送之后, 攻击者会等待一段合适的时间 D_A 再次发送, 从全局时间的角度来说, 从式(6)

可得

$$T_{i+1}^\alpha - T_i^\alpha = (t_{i+1} - t_i) + (D_{i+1}^\alpha - D_i^\alpha) \quad (7)$$

其中, 验证点 O_α 第一次接收目标车辆消息的时间 $T_{i+1}^\alpha = T_i + D_A + D_A^\alpha$, 第二次接收目标车辆消息的时间 $T_i^\alpha = T_i + D_A^\alpha$, 且 $T_{i+1} = T_i + D_A$ 。如果存在攻击者, 从攻击者的位置发送消息到验证点 O_α 的传播时延为 $D_A^\alpha = (p_\alpha - p_o) / v_r$, 由式(7)推导出

$$D_A = (t_{i+1} - t_i) + (D_{i+1}^\alpha - D_i^\alpha) \quad (8)$$

只存在一个验证点的情况下,当攻击者离验证点足够近,可以通过设置发送两次消息之间的间隔时间 D_A 进行欺骗攻击,对单个验证点进行消息时间戳伪造攻击如图 3 所示。

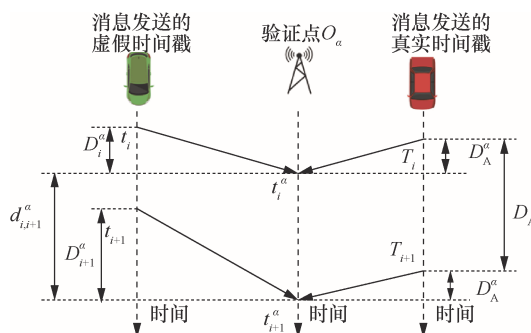


图3 对单个验证点进行消息时间戳伪造攻击
Figure 3 Attack with forged timestamps on a single verifier

(2) 抗载波频率操纵攻击的安全性分析

在图 1 中, 当只有一个验证点 O_a 接收车辆消息时, 由式(5)可以得出结论, 攻击者只需将载波频率 f_1 调整为 f_a , 验证点 O_a 接收消息信号的频率是预期信号频率 f_c , 攻击不会被检测到。

3.2 基于两个验证点的安全性分析

(1) 抗时间戳伪造攻击的安全性分析

当验证点数量为 2 时, 攻击者的目标是需要调整发送 M_i 和 M_{i+1} 的时间间隔 $D_{i,i+1}$, 车辆消息 M_i 和 M_{i+1} 需要经过两个不同的传播时延 D_A^α 和 D_A^β 分别到达两个验证点 O_α 和 O_β 。因此攻击者仍然需要 D_A 满足式(8)和式(9)才能成功发起攻击。

$$D_A = (t_{i+1} - t_i) + (D_{i+1}^\beta - D_i^\beta) \quad (9)$$

由式(8)和式(9)可推导出

$$D_{i+1}^\alpha - D_i^\alpha = D_{i+1}^\beta - D_i^\beta \quad (10)$$

对于车辆消息 M_i ，攻击者可以任意选择 p_i

进行欺骗攻击,然而,对于另一条车辆消息 M_{i+1} ,攻击者需要精心构造车辆消息中的位置 p_{i+1} 使得式(9)成立,由于消息的传播时延和距离相关,将式(10)重写为关于距离的公式,位置 p_{i+1} 由位置 p_i 、验证点位置 p_α 和 p_β 决定。定义集合 $P(p_i, p_\alpha, p_\beta) = \{p \in \mathbb{R}^n \mid \|p - p_\alpha\| - \|p - p_\beta\| = \|p_i - p_\alpha\| - \|p_i - p_\beta\|\}$, 其中 n 是维度的数量。攻击者可以选择任意一个属于集合 $P(p_i, p_\alpha, p_\beta)$ 中的位置 p_{i+1} 来完成攻击。当 $n=2$ 时,即在二维情况下,集合 $P(p_i, p_\alpha, p_\beta)$ 对应于双曲线上的一条臂,且此双曲线上任意一点到焦点的距离差为 $\|p_i - p_\alpha\| - \|p_i - p_\beta\|$, 因此当车辆消息 M_{i+1} 中的位置 p_{i+1} 对应此双曲线上一条臂中的某个位置时,就可以质疑其是虚假的车辆轨迹。

(4) 抗载波频率操纵攻击的安全性分析

对两个验证点进行载波频率操纵攻击如图4所示,攻击者对两个验证点发起攻击。由于验证点根据式(5)验证载波频率,从攻击者角度来看,攻击者需要依据此公式计算出来一个特殊的车辆位置,该位置可以使得不同方向上的径向速度都相同,从而使得两个验证点接收到同样的载波频率。为了欺骗验证点,攻击者需要调整消息广播的载波频率 f_1 , 使得到达每个验证点真实的载波频率 f_B 满足以下条件:

$$f_B = \frac{f_1}{1 - v_i^\alpha / v_c} \quad (11)$$

$$f_B = \frac{f_1}{1 - v_i^\beta / v_c} \quad (12)$$

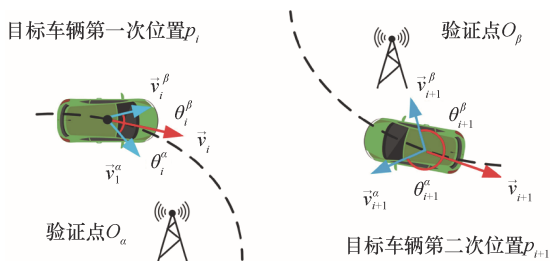


图4 对两个验证点进行载波频率操纵攻击

Figure 4 Attack with carrier frequency manipulation on two verifiers

这使得 $v_i^\alpha = v_i^\beta$, 即 $\theta_i^\alpha = \theta_i^\beta$ 。车辆速度 $\vec{v}_i$ 应平分矢量 $\vec{v}_i^\alpha$ 和 $\vec{v}_i^\beta$ 形成的夹角。从几何的角度来说, 车辆消息 $M_i = (\vec{v}_i, p_i, t_i)$ 中的 $\vec{v}_i$ 应与以 p_α 和

p_β 为焦点的双曲线中的一条臂相切, 该双曲线的半长轴长度为从 p_i 到焦点距离差的一半。因此当车辆消息 M_{i+1} 中的位置 p_{i+1} 对应此双曲线上一条臂中的某个位置时, 就可以质疑其是虚假的车辆轨迹。

3.3 基于3个验证点的安全性分析

(1) 抗时间戳伪造攻击的安全性分析

当验证点数量为3时, 由上文的结论得出以下关系式。

$$D_{i+1}^\alpha - D_i^\alpha = D_{i+1}^\beta - D_i^\beta = D_{i+1}^\gamma - D_i^\gamma \quad (13)$$

两条车辆消息 M_i 和 M_{i+1} 分别被发送到3个验证点 O_α 、 O_β 、 O_γ , 使得 p_i 和 p_{i+1} 需要满足以下条件。

$$p_{i+1} \in \bigcap_{\substack{\{O_\alpha, O_\beta, O_\gamma\} \in V \\ O_\alpha \neq O_\beta}} P(p_i, p_\alpha, p_\beta) \quad (14)$$

即需要3条不同的双曲线构成平面上的交点。为了方便表示, 令 $l_\alpha = \sqrt{(x - x_\alpha)^2 + (y - y_\alpha)^2}$, $l_\beta = \sqrt{(x - x_\beta)^2 + (y - y_\beta)^2}$, $d_{\alpha\beta}(p_i) = \|p_i - p_\alpha\| - \|p_i - p_\beta\|$, $l_\gamma = \sqrt{(x - x_\gamma)^2 + (y - y_\gamma)^2}$, $d_{\alpha\gamma}(p_i) = \|p_i - p_\alpha\| - \|p_i - p_\gamma\|$, 并且两条双曲线 $P(p_i, p_\alpha, p_\beta)$ 和 $P(p_i, p_\alpha, p_\gamma)$ 的交点 $(x, y) \in \mathbb{R}^2$ 必须满足

$$l_\alpha - l_\beta = d_{\alpha\beta}(p_i) \quad (15)$$

$$l_\alpha - l_\gamma = d_{\alpha\gamma}(p_i) \quad (16)$$

从式(15)、式(16)可得

$$b \cdot x + c \cdot y + g + h = 0 \quad (17)$$

其中, b 、 c 、 g 、 h 都是常量。

$$b = \frac{x_\alpha(d_{\alpha\gamma}(p_i) - d_{\alpha\beta}(p_i)) - x_\beta d_{\alpha\gamma}(p_i) + x_\gamma d_{\alpha\beta}(p_i)}{d_{\alpha\beta}(p_i)d_{\alpha\gamma}(p_i)},$$

$$c = \frac{y_\alpha(d_{\alpha\gamma}(p_i) - d_{\alpha\beta}(p_i)) - y_\beta d_{\alpha\gamma}(p_i) + y_\gamma d_{\alpha\beta}(p_i)}{d_{\alpha\beta}(p_i)d_{\alpha\gamma}(p_i)},$$

$$g = \frac{x_\beta^2 + y_\beta^2 - x_\alpha^2 - y_\alpha^2 + d_{\alpha\beta}(p_i)^2}{2d_{\alpha\beta}(p_i)},$$

$$h = \frac{x_\alpha^2 + y_\alpha^2 - x_\gamma^2 - y_\gamma^2 - d_{\alpha\gamma}(p_i)^2}{2d_{\alpha\gamma}(p_i)}.$$

将式(17)代入式(15)或式(16), 可得到一个二元一次方程, 产生 0、1 或 2 个交点, 即 0、1 或 2 个解。由定义可知, 3 条双曲线至少有一个焦点 p_i , 攻击者为了获得满足式(4)的虚假位置, 最多只能有一个可能的位置来欺骗验证点。当验证点数量为 3 时, 针对位置 p_i 形成的双曲线如图 5 所示, 攻击者最多只能构造一个虚假位置对验证点实施欺骗攻击, 因此利用 3 个验证点可以完全实现车辆消息中的轨迹验证。

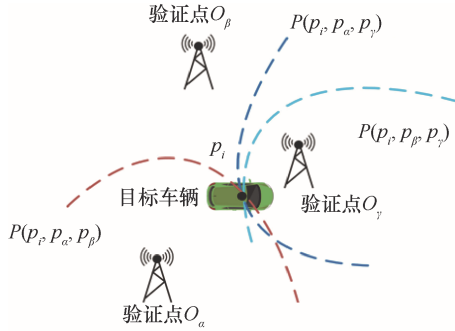


图 5 当验证点数量为 3 时, 针对位置 p_i 形成的双曲线
Figure 5 Pairwise hyperbolas for position p_i with three verifiers

(2) 抗载波频率操纵攻击的安全性分析

由上文可以得出结论: 此攻击满足 $v_i^\alpha = v_i^\beta = v_i^\gamma$ 。攻击者需要使车辆消息 M_i 中的位置 p_i 位于任意一条两两验证点连接的直线上, 从几何的角度来说, 矢量 $\vec{v}_i$ 无法平分 $\vec{v}_i^\alpha$ 、 $\vec{v}_i^\beta$ 和 $\vec{v}_i^\gamma$ 两两形成的夹角, 使得 $\theta_i^\alpha = \theta_i^\beta = \theta_i^\gamma$, 因此当 3 个验证点不位于同一方向的前提下, 攻击者无法发起载波频率操纵攻击。

综上所述, 如果在验证过程中方案满足下列条件, 可以探测到欺骗攻击。

如果 $|V| \geq n$, 且 $\exists_{p_i, p_{i+1} \in M_i} p_{i+1} \notin P(p_i, p_\alpha, p_\beta)$, 其中 n 为车辆的位置维度数量, 即 $p_i \in \mathbb{R}^n$, 则至少有 n 个验证点接收到车辆消息, 每个验证点接收到两个不同的车辆消息, 且其中的一条车辆消息显示车辆位置不对应双曲线 $P(p_i, p_\alpha, p_\beta)$ 一条臂上的任意位置。

如果 $|S| \geq 3$, 且 $|O| \geq n+1$, 则至少有 $n+1$ 个验证点接收到车辆消息, 且每个验证点接收到至少 3 条车辆消息, 这些车辆消息组成了一条完整的车辆轨迹。

4 实验结果与分析

为了验证所提方案的有效性和高效性, 基于目前已有的硬件, 本文采用蔚来 ES8 作为目标车辆。

目标车辆的通信模块如图 6 所示, 本文基于 LTE-V 通信协议选择载波频率 5.2 GHz 进行实验, 该车的通信模块搭载中兴 ZM8350 车载模组, 通过车载 GPS 接收机 Pwrpak E1 进行精确定位, 使用 USRP B210 无线电台发射信号, 并利用 VERT 2450 天线进行广播。目标车辆与各验证点的实物图如图 7 所示。验证点包括路侧单元、基础设施和可信的周围车辆。其中, 路侧单元和基础设施已安装 CPU/MPU、LTE-V 通信模块、定位设备等^[18-22]。可信车辆安装与目标车辆相同的通信模块, 与目标车辆进行通信。

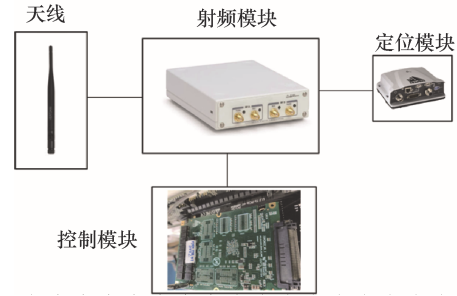


图 6 目标车辆的通信模块
Figure 6 Communication module on the target vehicle

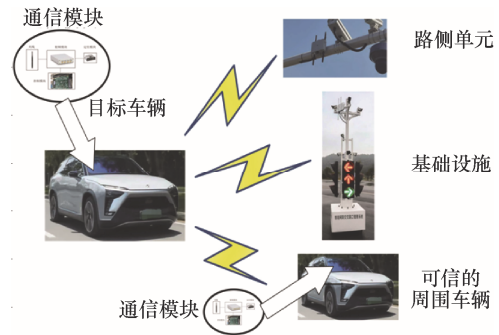


图 7 目标车辆与各验证点的实物图
Figure 7 Physical view of the target vehicle and verifiers

由式(4)可得, 攻击者需要精确设置两次车辆消息传输的间隔时间才能进行有效攻击, 因而本文方案决定随机地设置攻击者的位置, 以便两次车辆消息到达各个验证点时的间隔时间满足攻击要求, 同时采用 SVM 方案^[5]作为对照

实验。

由于车辆的体积大，存在定位误差，并且由于时间测量误差、信道噪声等，阈值 τ_1 和 τ_2 需要在实验前期根据错误拒绝率与错误接受率来选择阈值，以便后续进行实验。设置阈值 τ_1 和 τ_2 如图8和图9所示，当错误拒绝率与错误接受率都相对较低时，此时阈值 $\tau_1 = 0.35\text{ s}$ 、 $\tau_2 = 15\text{ Hz}$ ，因而本文选择将阈值 τ_1 、 τ_2 分别设置成 0.35 s 、 15 Hz 。

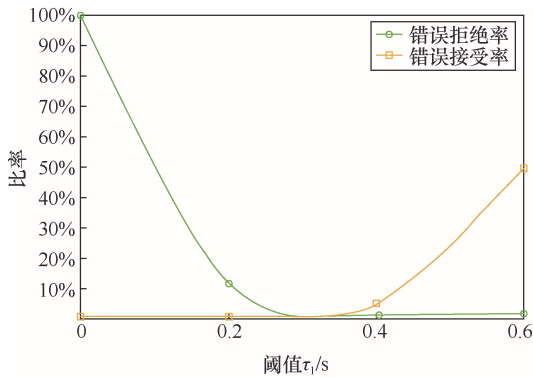


图8 设置阈值 τ_1
Figure 8 Setting the first threshold τ_1

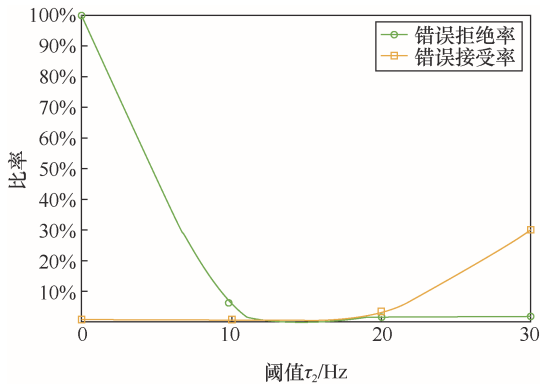


图9 设置阈值 τ_2
Figure 9 Setting the second threshold τ_2

不同数量验证点的情况下本文方案的正确率如图10所示，可以看出，当验证点数量从1增加至3时，本文方案验证的正确率显著上升；当验证点数量为4或5时，验证的正确率无明显变化，这表明随着验证点数量的增加，验证正确率会上升，当验证点数量为4或5时，正确率达到饱和，与第3节的安全性分析一致。因此，后续实验只设置3个验证点。

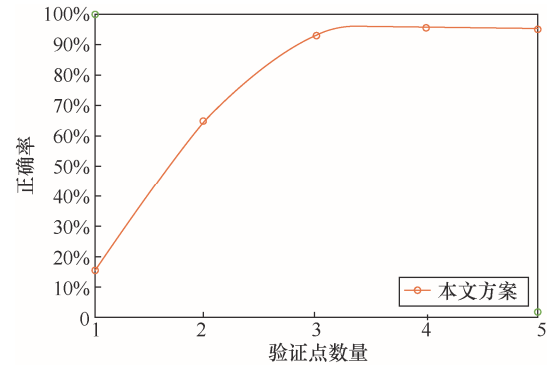


图10 不同数量验证点的情况下本文方案的正确率
Figure 10 The accuracy of proposed scheme with different numbers of verifiers

两种方案验证真实车辆轨迹的正确率如图11所示。此次实验将车辆轨迹全部设置为真实的车辆轨迹，随着目标车辆发送的车辆消息数量逐渐增多，验证车辆轨迹的正确率也逐渐上升，最终接近94.50%，这表明本文方案在验证车辆轨迹时具有一定的有效性。此外当车辆消息数目少于40时，本文方案验证车辆轨迹的正确率增长速率快，表明本文方案能够在很短时间内达到良好的车辆轨迹验证作用。此外，本文方案的验证正确率始终优于SVM方案，这是因为SVM方案需接收到反射信号进行车辆轨迹验证，如果设置的反射点较少，验证轨迹的正确率就会较低。

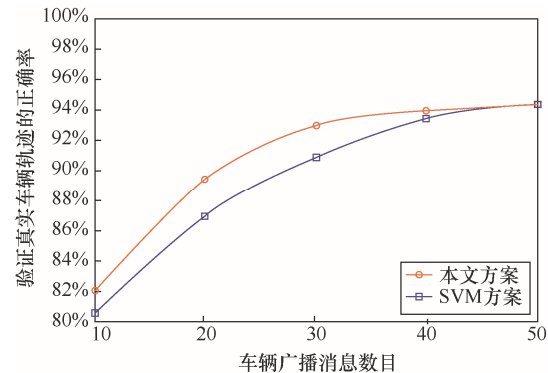


图11 两种方案验证真实车辆轨迹的正确率
Figure 11 The two schemes verify the accuracy of true vehicle track

两种方案验证虚假车辆轨迹的正确率如图12所示，该实验中，本文方案将目标车辆发送的车辆轨迹全部设置为虚假的车辆轨迹，随着目标车辆发送的车辆消息逐渐增多，验证车辆轨迹的正确率逐渐上升，最终接近94.00%，这表明本文方案并没有

受到虚假车辆轨迹的干扰,成功实现了抗时间戳伪造攻击和抗载波频率操纵攻击。

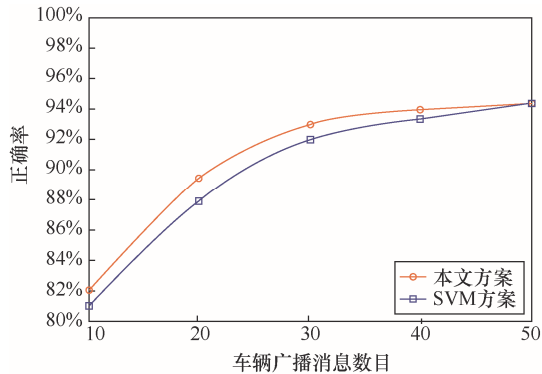


图12 两种方案验证虚假车辆轨迹的正确率
Figure12 The two schemes verify the accuracy of false vehicle track

本文方案验证车辆轨迹的错误接受率和错误拒绝率如图13所示。错误接受率指的是方案将虚假车辆轨迹验证为真实车辆轨迹的比率。错误拒绝率指的是方案将真实车辆轨迹验证为虚假车辆轨迹的比率,出现这些情况可能是在实验环境中存在时间测量误差或者信道噪声等。从图13可以看出,随着目标车辆消息数量逐渐增加,错误接受率和错误拒绝率逐渐下降,同时当目标车辆消息数量从10增加至30时,实验结果比率曲线下降迅速,这表明本文方案在验证目标车辆轨迹时具有高效性。在不同数量的目标车辆情况下,本文方案的验证时间如图14所示。随着车辆数量逐渐增多,验证点接收到的车辆消息也逐渐增多,验证时间变长,如何控制并缩短验证时间,将是车辆轨迹验证领域的一个重要方向。

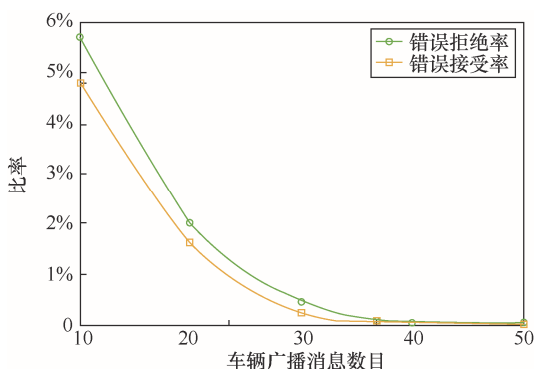


图13 本文方案验证车辆轨迹的错误接受率和错误拒绝率
Figure 13 The proposed scheme verify vehicle track's false acceptance and rejection rates

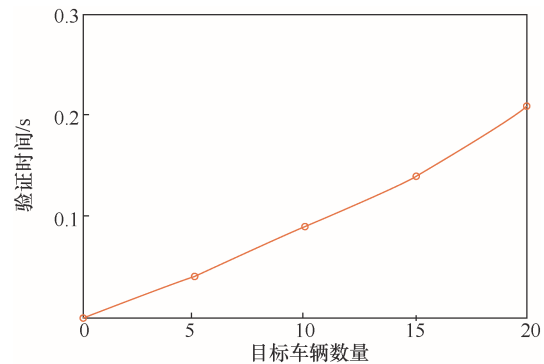


图14 本文方案的验证时间
Figure 14 The verification time of proposed scheme

5 结束语

基于同一广播通信信道,本文提出了一种抗时间戳伪造攻击和抗载波频率操纵攻击的轻量级车辆轨迹安全验证方案。该方案基于智能汽车已有的硬件,无须部署任何新的硬件,减少了汽车成本开销,实现了对智能汽车车辆轨迹的安全验证。在时间不同步的情况下,每个验证点计算消息接收时间与发送时间戳的时间间隔,通过联立两两验证点的时间间隔所形成的空间位置约束方程,达到了抗时间戳伪造攻击的防御效果。基于多普勒效应,每个验证点计算消息到达频率和预定发射频率的频偏,通过联立两两验证点的频偏所形成的速度矢量约束方程,实现了抗载波频率操纵攻击的安全目的。最后的安全性分析和实验结果验证了该方案的安全性和可行性。下一步工作将聚焦于优化处理海量车辆轨迹数据的验证过程,以确保实时结果的准确性。

参考文献:

- [1] DE-BRUHL B, WEERAKODY S, SINOPOLI B, et al. Is your commute driving you crazy: a study of misbehavior in vehicular platoons[C]//Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. 2015: 1-11.
- [2] PI W, YANG P T, DUAN D L, et al. Malicious user detection for cooperative mobility tracking in autonomous driving[J]. IEEE Internet of Things Journal, 2020, 7(6): 4922-4936.
- [3] LEON F, GAVRILESCU M. A review of tracking and trajectory prediction methods for autonomous driving[J]. Mathematics, 2021, 9(6): 660.
- [4] DONGRE S, RAHBARI H. Message sieving to mitigate smart gridlock attacks in V2V[C]//Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2021: 129-134.

- [5] SUN M S, MAN Y M, LI M, et al. SVM: secure vehicle motion verification with a single wireless receiver[C]//Proceedings of the 13th ACM Conference on Security & Privacy in Wireless and Mobile Networks. 2020: 65-76.
- [6] DE-MEO P, MESSINA F, POSTORINO M N, et al. A reputation framework to share resources into IoT-based environments[C]//IEEE 14th International Conference on Networking Sensing and Control. 2017: 513-518.
- [7] GROZA B, MURVAY P S. Security solutions for the controller area network: bringing authentication to in vehicle networks[J]. IEEE Vehicular Technology Magazine, 2018, 13(1): 40-47.
- [8] SUN M S, LI M, GERDES R. Verification and inference of positions in vehicular networks through anonymous beaconing[J]. IEEE Transactions on Mobile Computing, 2014, 13(10): 2415-2428.
- [9] YAN G J, CHOUDHARY G, WEIGLE M C, et al. Providing VANET security through active position detection[C]//Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks. 2007: 73-74.
- [10] DU C L, ZHANG R D, LOU W J, et al. Mob track: locating indoor interfering radios with a single device[C]//IEEE INFOCOM 2016: 1-9.
- [11] KOOPMAN P, WAGNER M. Autonomous vehicle safety: an interdisciplinary challenge[J]. IEEE Intelligent Transportation Systems Magazine, 2017, 9(1): 90-96.
- [12] SANDERS C, WANG Y Q. Localizing spoofing attacks on vehicular GPS using vehicle-to-vehicle communications[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15656-15667.
- [13] BAKER R, MARTINOVIC I. Secure location verification with a mobile receiver[C]//Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy. 2016: 35-46.
- [14] YAO Y, XIAO B, WU G f, et al. A novel sybil attack detection method based on RSSI for VANET[C]//IEEE International Conference on Dependable Systems and Networks. 2017: 591-602.
- [15] SUN M S, LI M, GERDES R. A data trust framework for VANET: enabling false data detection and secure vehicle tracking[C]//IEEE Conference on Communications and Network Security. 2017: 1-9.
- [16] DE-MEO P, MESSINA F, POSTORINO M N, et al. A reputation framework to share resources into IoT-based environments[C]//IEEE 14th International Conference on Networking Sensing and Control. 2017: 513-518.
- [17] SUN M S. Secure motion claim verification and decision-making for vehicular cyber-physical systems[D]. Arizona: University of Arizona, 2021.
- [18] LEINMULLER T, SCHOCH E, KARGL F. Position verification approaches for vehicular ad hoc networks[J]. IEEE Wireless Communications Magazine, 2006, 13(5): 16-21.
- [19] WONG W E, LI X L, LAPLANTE P A. Be more familiar with our enemies and pave the way forward: a review of the roles bugs played in software failures[J]. Journal of Systems and Software, 2017, 133(11): 68-94.
- [20] LI C L, FU Y C, RICHARD F YU, et al. Vehicle position correction: a vehicular blockchain networks-based GPS error sharing framework[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(2): 898-912.
- [21] LI F N, CHANG L B. MEKF with navigation frame attitude error parameterization for INS/GPS[J]. IEEE Sensors Journal, 2020, 20(3): 1536-1549.
- [22] RANGANATHAN A, ÓLAFSDÓTTIR H, CAPKUN S. SPREE: a spoofing resistant GPS receiver[C]//Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking. 2016: 348-360.

[作者简介]



宁志强 (1997-), 男, 安徽池州人, 中国科学技术大学硕士生, 主要研究方向为车辆轨迹安全验证。

汪媛媛 (1995-), 女, 安徽桐城人, 中国科学技术大学博士生, 主要研究方向为临近空间网络、网络优化。

张驰 (1977-), 男, 广西百色人, 博士, 中国科学技术大学副教授, 主要研究方向为无线网络、网络安全和区块链技术。

魏凌波 (1979-), 女, 陕西周至人, 博士, 中国科学技术大学副研究员, 主要研究方向为应用密码学和区块链技术。

俞能海 (1964-), 男, 安徽无为, 中国科学技术大学教授、博士生导师, 主要研究方向为视频处理与多媒体通信、信息检索、媒体内容安全。

HAO Yue (1987-), 男, 博士, 旧金山州立大学副教授, 主要研究方向为无线网络和网络安全。