国 际 电 信 联 盟

ITU-T X.1372

(03/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务(2) – 智能交通系统（ITS）安全

车联网（V2X）通信的安全导则

ITU-T X.1372建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	**X.1370–X.1389**
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1372建议书

车联网（V2X）通信的安全导则

摘要

ITU-T X.1372建议书为车联网（V2X）通信系统提供安全导则。V2X是本建议书中讨论的、有关车辆对车辆（V2V）、车辆对基础设施（V2I）、车辆对漫游设备（V2D）以及车辆对行人（V2P）通信模式的一个通用术语。

过去几年间，在智能交通系统（ITS）环境中的车载通信领域取得了巨大发展。V2X通信显著提高了道路安全、减少了交通拥堵并增加了便利性。然而，V2X通信也使得智能交通系统环境中的相关实体容易受到各种形式的网络攻击。

为了解决这一安全问题，本建议书确定V2X通信环境中的威胁，规定V2X通信的安全要求，以缓解这些威胁。本建议书还描述可能的安全V2X通信的实施方案。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1372	2020-03-26	17	11.1002/1000/14091

关键词

智能交通系统（ITS）安全、风险分析、安全要求、威胁分析、V2I、V2V、V2D、V2P、V2X。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1372建议书

车联网（V2X）通信的安全导则

1 范围

本建议书为车联网（V2X）通信提供安全导则。V2X是本建议书中讨论的、有关车辆对车辆（V2V）、车辆对基础设施（V2I）、车辆对漫游设备（V2D）以及车辆对行人（V2P）通信模式的一个通用术语。本建议书确定V2X通信环境中的威胁，规定V2X通信的安全要求，并描述可能的安全V2X通信的实施方案。

特定的 V2X 通信安全控制不在本建议书的讨论范围内。

2 参考文献

下列 ITU-T 建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T 建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 可核查性（accountability）[b-ITU-T X.800]：实体的一种属性，用于确保实体的行动可被唯一地追溯至该实体。

3.1.2 真实性（authenticity）[b-ITU-T X.641]：保护相互验证和数据来源验证。

3.1.3 验证（authentication）[b-ITU-T X.1252]：对实体与所呈现身份之间关联性实现充分信任的过程。

注 – 在 IdM 语境内使用术语认证是指实体认证。

3.1.4 授权（authorization）[b-ITU-T X.800]：授予权限，包括授予基于访问权限进行访问的权限。

3.1.5 可用性（availability）[b-ITU-T X.800]：经授权实体一旦需要即可访问和使用的属性。

3.1.6 认证机构（certification authority）(CA) [b-ITU-T X.509]：被一个或多个实体所信任的机构，用于创建和以数字方式签署公开密钥证书。可选地，认证机构可以创建对象的密钥。

3.1.7 机密性（confidentiality）[b-ITU-T X.800]：使信息不泄漏给未授权的个人、实体或过程或者不使信息为其利用的特性。

3.1.8 完整性（integrity）[b-ITU-T X.800]：数据未经授权而被更改或销毁的属性。

3.1.9 消息验证码（message authentication code）（MAC）[b-ITU-T X.813]：用于提供数据来源验证和数据完整性的密码检查值。

3.1.10 漫游设备（nomadic device）[b-ITU-T F.749.1]：漫游设备包括所有类型的信息通信设备以及娱乐设备，驾驶者和/或乘客可将之带入车辆以在驾驶时使用。例子包括移动电话、便携式计算机、平板电脑、移动导航设备、便携式媒体播放器和多功能智能电话。

3.1.11 带来源证明功能的不可否认性（non-repudiation with proof of origin）[b-ITU-T X.800]：为数据的接收方提供数据来源的证明。这将防止发送方虚假否认其曾发送过数据或其内容的任何企图。

3.1.12 化名（pseudonym）[b-ITU-T X.1252]：与实体的关系未知或仅在其所用语境小范围内知晓的标识符。

注 – 使用化名可以避免或减少与使用标识符绑定相关的隐私风险，标识符绑定可能会暴露实体的身份。

3.1.13 公开密钥证书（public-key certificate）（PKC）[b-ITU-T X.509]：一个实体的公开密钥，以及其他一些信息，利用发放它的认证机构（CA）的私钥，通过数字签名而变得不可伪造。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 不当行为（misbehavior）：导致设备发送错误信息的行为，这可能导致其他设备采取错误的行动；或者设备尽管收到了正确的信息，但仍采取了错误的行动。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

AES 高级加密标准

AVN 音频、视频和导航

CA 认证机构

CAMP 防撞指标合作伙伴（CAMP 联盟）

CCM 带有密码块链接消息验证码的计数器模式

CCU 中央通信单元

DDoS 分布式拒绝服务（攻击）

EEBL 电子紧急制动灯

ECDSA 椭圆曲线数字签名算法

ECIES 椭圆曲线综合加密方案

ECU 电子控制单元

GPS 全球定位系统

HDMI 高清多媒体接口

ID 标识符

ITS 智能交通系统

IVN 车载网络

KDF	密钥派生函数
LDM	本地动态地图
LOS	视线
LTE	长期演进
MAC	消息验证码
MHL	移动高清链路
NFC	近场通信
NGN	下一代网络
NLOS	非视线
OBD	车载诊断
OBU	车载单元
PII	个人可识别信息
PKI	公开密钥基础设施
QoS	服务质量
RSU	路侧单元
SCMS	安全证书管理系统
SHA	安全哈希算法
USB	通用串行总线
V2I	车辆到基础设施
V2D	车辆到漫游设备
V2P	车辆到行人
V2V	车辆到车辆
V2X	车辆到万物
VGP	车载网关平台
VRU	弱势道路使用者
WAVE	车载环境中的无线访问
WiFi	无线保真

5 惯例

无。

6 V2X通信

6.1 概述

智能交通系统（ITS）包括旨在提高交通系统安全性和效率的众多信息通信技术。在过去的几年中取得了重大发展，特别是在车载通信系统方面。

车载通信系统支持车辆与车辆之间、车辆与基础设施之间以及车辆与漫游设备之间进行数据交换。数据类型包括当前位置、车辆速度和车载传感器发出的告警。另外，路侧单元（RSU）可以提供连接交通监控系统的通信链路，交通监控系统可以在周边车辆中收集和分发有关危险情况的告警。不过，如果没有安全保护，则 ITS 可能对交通安全以及人类生命构成危险。因此，目前正在对 ITS 的安全性开展调查研究，以确保 ITS 的安全和成功部署。

图 1 概述了车载通信。车载通信可分为车辆外部通信和车辆内部通信。车辆的内部网络称为车载网络（IVN），涉及诸如传感器和电子控制单元（ECU）等车辆部件。外部通信可以分为 V2V、V2I、V2D 和 V2P 通信。车载单元（OBU）指的是安装在车辆上的无线通信单元，而 RSU 指的是位于道路上的无线访问单元。基础设施由 RSU 和后端设施组成，例如交通管理、监视系统、认证机构（CA）。RSU 可以通过有线或无线网络连接到后端设施。

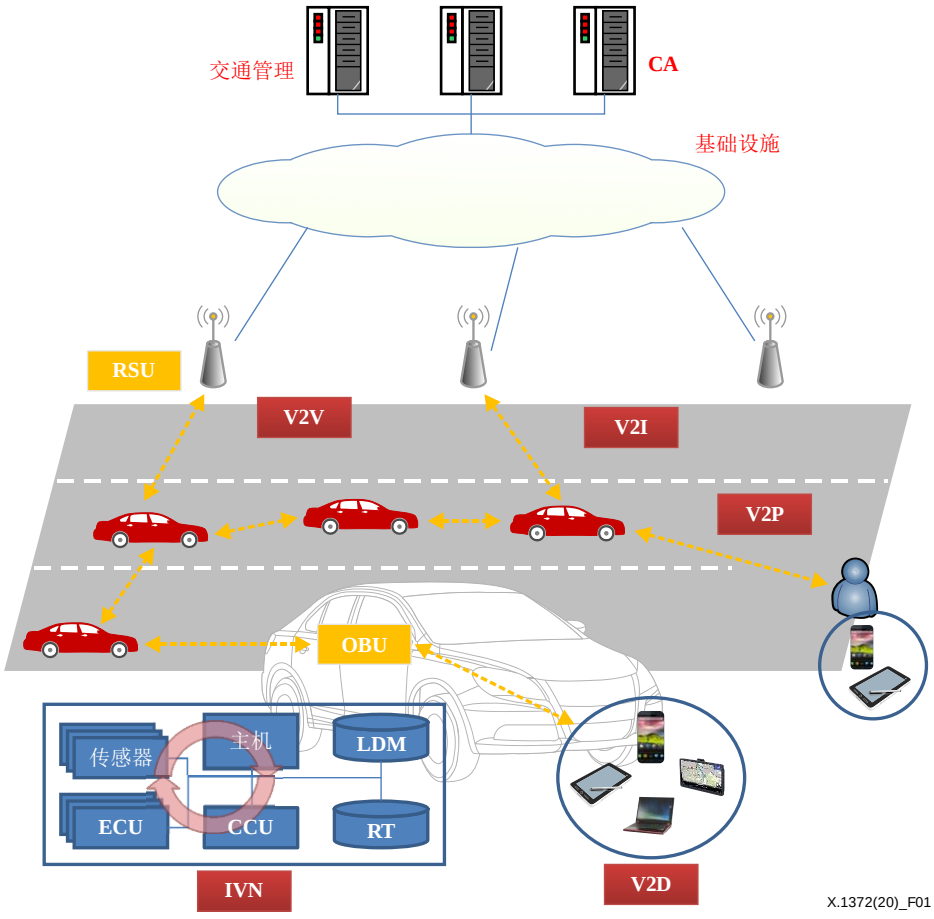


图1 – 车载通信概述

6.2 V2V通信

V2V 通信包括车辆与车辆之间数据的无线传输。V2V 通信的目的是通过在车辆与车辆之间共享和发送信息来防止事故发生。根据 V2V 技术的实施方式，车辆可能会收到告警，告知可能发生事故的风险。然后，车辆可以采取先发制人的动作，例如制动以减速。通过共享速度和路况，V2V 中的队列通信可以使组驾驶成为可能。此外，信标可以用于车辆与车辆之间的信息交换，以支持轻松与安全的驾驶。在 V2V 通信的支持下，车辆可以收集信息，包括对其周围环境的 360 度感知。

可确定以下 V2V 通信场景。

– V2V告警传播：

在V2V告警传播场景中，告警消息从一辆车传播到另一辆车。例如，如果发生交通事故，应向所有接近事故的车辆后向发送告警，告知前方发生碰撞。另一方面，如果应急车辆（例如警车）从车辆后面驶近，则告警消息应前向传输到附近和前方的所有车辆，以便应急车辆可以安全地高速驶近。图2具体显示了前向事故告警后向传播的情况，图3显示了应急车辆从后面驶来且告警消息前向传播的情况；

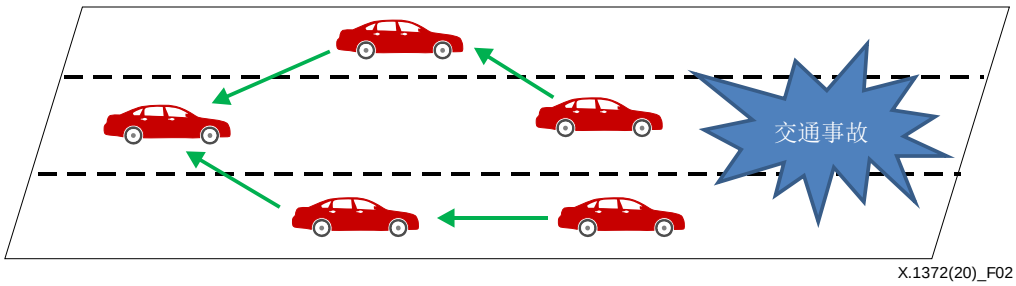


图2 – V2V告警传播 – 后向传播

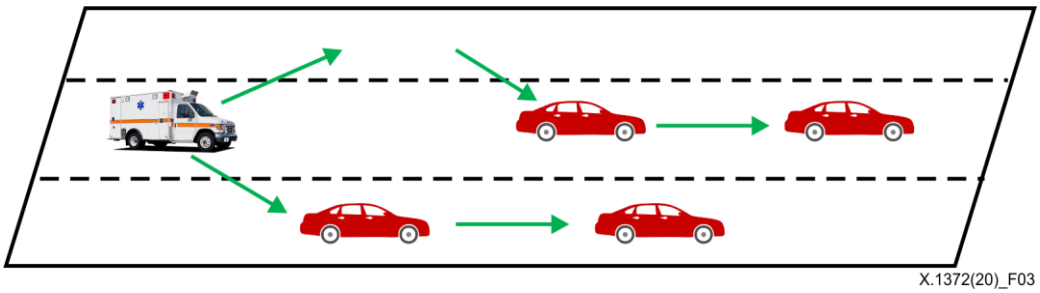


图3 – V2V告警传播 – 前向传播

– V2V队列通信：

在V2V队列通信场景中，几辆车组成一个组，它们可以在该组中相互通信。例如，沿同一路线或至少一段时间内保持同一路线的车辆可形成一个队列。该组可传递车辆状态信息，以帮助安全驾驶。图4具体显示了V2V队列通信；

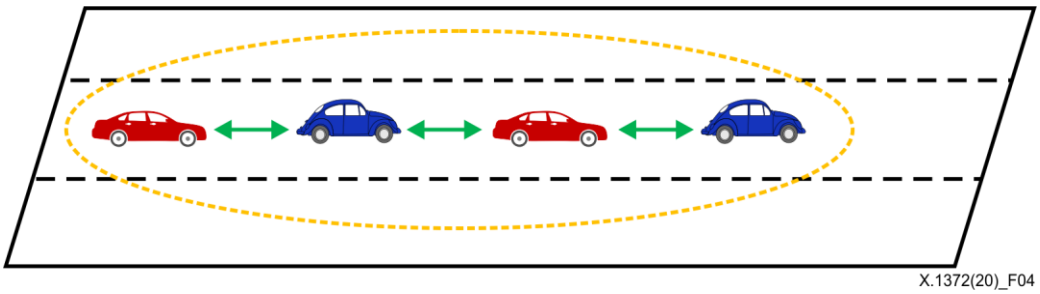


图4 – V2V队列通信

– V2V信标：

在V2V信标场景中，每辆车都会定期向附近的车辆发送其车辆状态信息，如当前速度、前进方向和位置。图5具体显示了V2V信标。

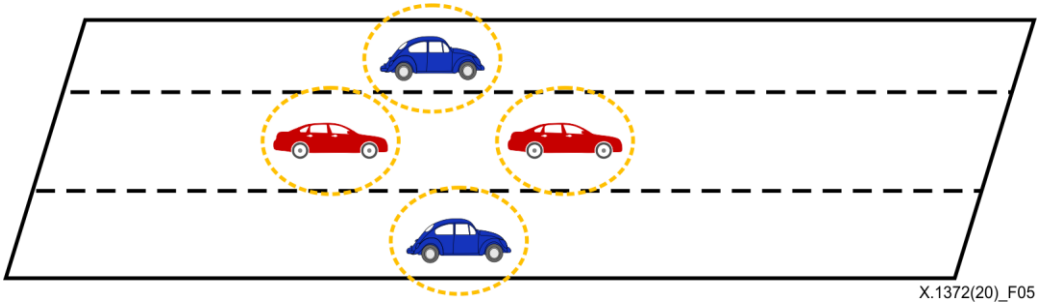


图5 – V2V信标

6.3 V2I通信

车辆到基础设施（V2I）通信指的是车辆与基础设施（如路侧单元（RSU））之间的无线数据传输。

可确定以下 V2I 通信场景。

– V2I告警：

V2I告警场景允许车辆与RSU等基础设施之间进行通信。例如，当在交叉路口发生交通事故时，RSU可以向即将驶近交叉路口的车辆发送告警消息。在右转或左转和汇合点进行车道进入协商的情况下，车辆接近的告警通知也是V2I告警用例。图6显示了V2I告警场景示例；

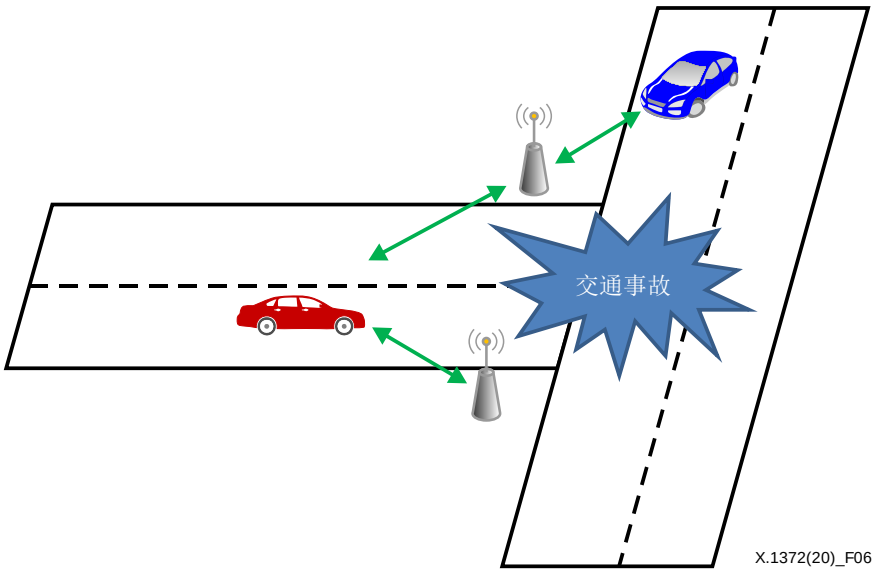


图6 – V2I告警

– V2I信息交换（包括V2V）：

V2I信息交换可以包括以下信息，例如车载标记/信息、交通信号灯的信号相位和时间信息、探查车辆数据、计费信息（例如收费站）、路面/天气/可见距离条件和道路建设信息。用例示例包括：

- 下载基本的交通数据：

  在ITS中，许多V2I消息可能包含告警消息。为了处理此类消息，车辆通常需要一张有关其所在位置或正在驶向何处的地图，或者可能需要车辆周围的实时情况信息。通常从诸如RSU之类的基础设施中下载此类信息；

- 支持交通效率的数据：

  在ITS中，车辆可以不定期地与基础设施进行通信，以获得与交通有关的信息，例如临时交通控制信息等。结果是，车辆可以知晓交通堵塞发生的位置。然后，它可以在基础设施的帮助下优化其路线，例如，通过连接移动网络的导航器更新其路线。因此，使用V2I通信可以提高车辆的效率。在另一个示例中，基础设施还可以基于车辆通过V2I通信提供的消息来更新交通信息。图7显示了V2I信息交换。

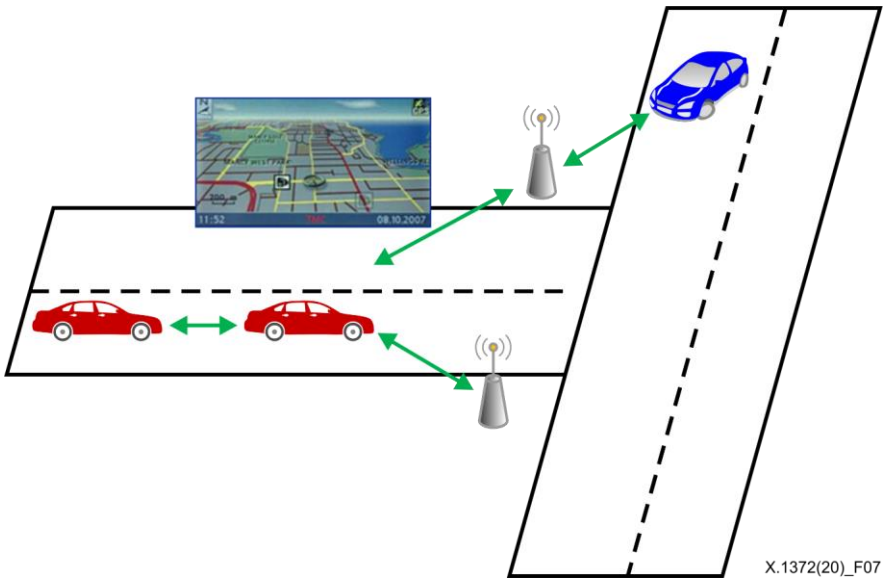


图7 – V2I信息交换

6.4 V2D通信

使用 V2D 通信技术，车辆与车辆中的智能电话、笔记本电脑和导航系统等移动设备相连，这通过具有连接汽车控制器局域网（CAN）总线的标准化接口的开放式体系结构来实现，或者通过将漫游设备之请求/响应转移到车辆上运行之系统的网关来实现。使用智能电话或移动设备，可以远程提供功能来确定和管理车辆状态信息，例如维护部件。另外，期待便利服务的进一步发展。

以旅行规划为例，驾驶者在漫游设备上选择目的地，然后漫游设备通过组合来自不同来源的不同信息项（例如公共交通工具的时间表（火车、地铁或公共汽车等））以及实时路况信息规划出一条路线来。车辆遵循规划的路线行进，如果交通状况发生短期变化，则绕行。漫游设备不仅可以做出有关机动的决策并执行决策，还可以对当地交通状况做出反应，例如跟随其他车辆、避开障碍物、改变车道以及在交通信号灯处停车等。漫游设备可以连接到车载网络。因此，攻击者可能会获得对车辆内部系统的访问权限。在通过蓝牙进行安全威胁的情况下，可以通过连接到车辆的智能电话上的应用程序执行恶意代码。车载音频、视频和导航（AVN）系统易遭受经由多媒体存储器的固件攻击，并容易经全球定位系统（GPS）或卫星无线电频道暴露于黑客攻击下。应控制通过漫游设备的攻击，以阻止车辆面临的安全风险。

以下讨论两种不同类型的 V2D 通信。

– 通过间接链路实现的V2D通信：

  车辆和漫游设备可以通过间接链路进行通信。通过间接链路进行通信意味着在最终节点之间存在提供通信的第三方设备（如接入点和路由器）。蜂窝电话和智能电话使用诸如长期演进（LTE）和Wi-Fi等移动无线宽带技术。为了与车辆进行通信，智能电话中无线保真（Wi-Fi）的使用正在增加。5G技术也是这些间接链路的一种关键通信信道。

– 通过直接链路实现的V2D通信：

  车辆和漫游设备可以通过直接链路进行通信，而无需在它们之间进行任何干预，也可以通过无线通信技术（如蓝牙、ZigBee和近场通信（NFC））进行通信。

车辆和漫游设备也可以通过有线链路进行通信。例如，漫游设备可以通过物理访问连接到车辆，例如通用串行总线（USB）、移动高清链路（MHL）和高清多媒体接口（HDMI）。车载诊断II（OBD-II）标准规定了诊断接口，还提供了车辆参数和数据传输过程的候选清单。

特别地，由于车辆与和行人相关的漫游设备进行通信，因此V2P通信可以被视为V2D通信的一种特例。

V2P方法适用于广泛的弱势道路使用者（VRU），包括非机动道路使用者，例如行人和骑自行车的人以及摩托车驾驶者和残疾人或行动不便的人。

由于涉及VRU的高级交通事故，ITS提出了通过传感器数据收集和感知及启用车辆与行人之间的信息交换等理念来增强道路安全的解决方案。更重要的是，V2P通信不仅会告警车辆驾驶者行人正在靠近以停下车辆，而且会提醒行人的移动电话以通知行人车辆正在驶近。

ITS可以检测VRU，并有助于防止车辆与VRU之间发生潜在的碰撞。图8显示了在驾驶者视线（LOS）场景中的行人，图9显示了不在驾驶者视线（NLOS）场景中的行人，用于演示ITS如何改善VRU道路安全性。

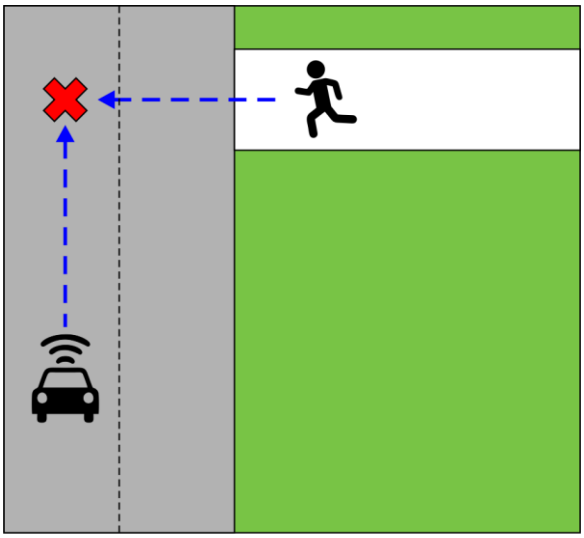


图 8 – LOS

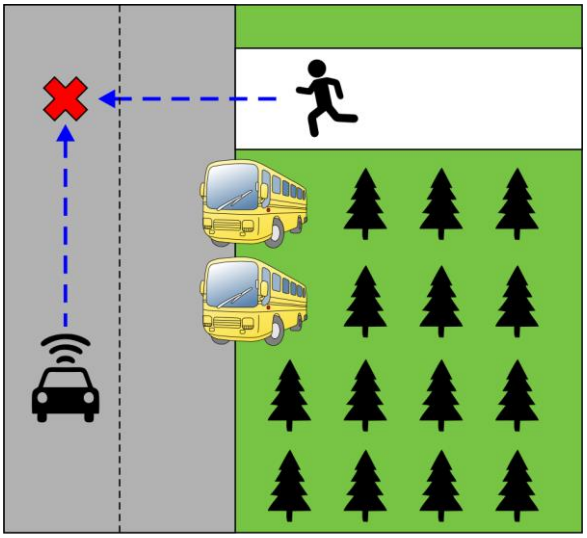


图 9 – NLOS

– 在驾驶者视线（LOS）中的行人：

如图8所示，诸如雷达、超声波传感器、激光测距仪和摄像机之类的有源传感器采用基于计算机视觉的方法，适用于从车辆看得见行人的地方来探测行人。当行人接近时，行驶中的车辆将检测到行人，而后做出关键决策。同时，车辆可以向行人的手机发出告警，提醒之潜在的危险；

– 不在驾驶者视线中（NLOS）的行人：

检测行人的能力受到传感器视野的限制。在图9中，行人被诸如树和停着的巴士等障碍物挡住了视线。但是，车载通信能够宣告和散布传感器视野之外的信息。一旦车辆收到告警通知，将更新其本地动态地图（LDM）并评估状况的严重性以做出决定。同时，行人的手机会收到告警通知。

7 已确定的威胁

7.1 对机密性的威胁

图10具体说明本节描述的对机密性威胁。

– 窃听：

攻击者可以嗅探（即，读取和/或记录）附近车辆的V2V消息和RSU的V2I消息，而后可以通过处理嗅探到的消息来分析交通信息。

攻击者可以嗅探中央通信单元与漫游设备之间的V2D消息。而后，攻击者可以分析有关车辆的动态信息，例如当前位置和速度。

攻击者可以嗅探V2P消息并误导行人进入危险的路况。

– 泄露个人身份信息：

攻击者可以通过收集车辆的V2X消息并跟踪特定人员在行驶路线上的位置来分析信息，以发现车辆的所有者。

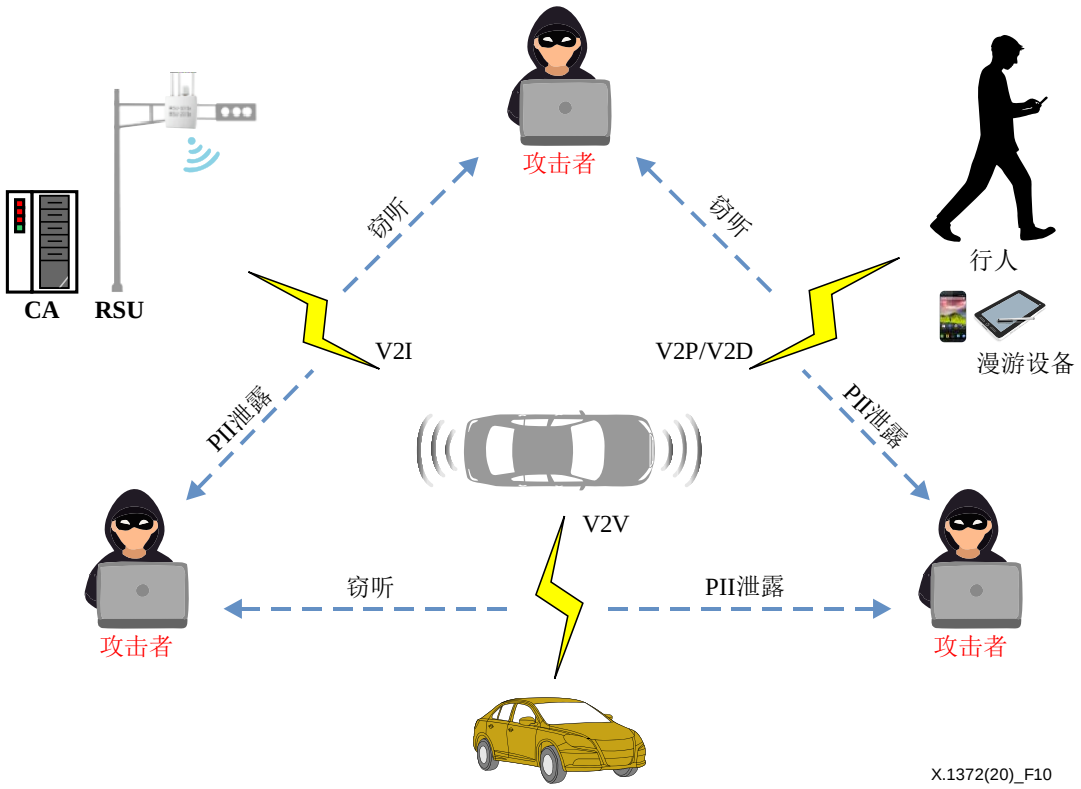


图10 – 对机密性的威胁

7.2 对完整性的威胁

图 11 具体说明本节描述的对完整性的威胁。

– 操纵路由消息：

恶意中间节点修改路由消息；车辆将收到虚假信息。

– 操纵证书信息：

操纵证书意味着修改车辆的私钥或ID（标识符），因此攻击者可以未经授权地使用另一辆车的证书信息。

– 操纵传感器信息：

攻击者可以修改通信模块的物理地址，或者可以操纵ECU信息，例如速度传感器。此外，车辆上有很多其他传感器，例如雷达和摄像头，作为驾驶者的辅助设备。错误的传感器数据（包括纬度、经度、海拔、速度、航向、方向盘角度和加速度）可能会传递到其他OBU或RSU。这一被操纵的传感器数据可造成交通混乱。例如，错误的加速度值可能会使附近的车辆打开其电子紧急制动灯（EEBL），以减少发生多车辆碰撞的机会，即使实际的交通状况很好。

– 操纵漫游设备上的应用：

一个被操纵的应用程序可通过V2D通信接口对车辆产生有害的影响。例如，被操纵的应用程序可迫使漫游设备向车辆发送大量的良性消息；这种行为称为消息泛滥。此外，被操纵的应用程序可将恶意代码注入OBU并发送一条需要大量计算资源的消息。被操纵的应用程序还可发送比OBU上可用存储容量大得多的大量消息。

– 重播攻击：

攻击者可拦截来自附近车辆的V2V消息和RSU的V2I消息。之后，该攻击者可出于恶意目重播这些消息或信息。

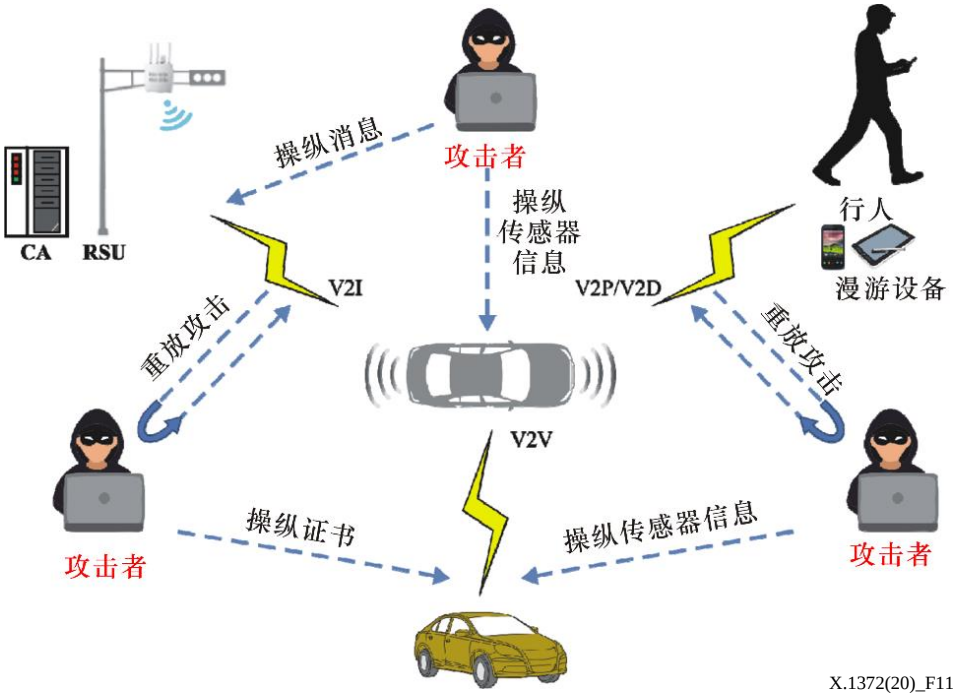


图11 – 对完整性的威胁

7.3 对可用性的威胁

图 12 具体说明本节描述的对可用性的威胁。

– 对V2X通信信道的干扰和分布式拒绝服务（DDoS）攻击：

攻击者可以发送许多无用的消息，该技术称为消息泛滥。路由节点仅转发特定的消息可归类为这种攻击。

– 对OBU的DDoS攻击：

攻击者可将恶意代码注入OBU，并发送需要大量计算资源的消息。该攻击者还可发送许多消息，这些消息的大小累计大于OBU的存储容量。特别地，未经授权的频繁软件更新就是此类严厉攻击的一个例子。

– 时序攻击：

时序攻击指的是诸如延迟向其他车辆发送安全性消息的攻击。因此，它可能会阻止适当的V2X通信服务，例如告警消息的广播。

– 对传感器的黑客攻击：

传感器可能受到攻击并导致故障以提供恶意值。通常，传感器中可能存在两种故障类型：瞬时故障和永久故障。系统正常运行期间可能会发生瞬时故障，并很快消失。实际上，大多数传感器都具有瞬时故障模型，该模型会限制提供错误测量值的时间。例如，GPS暂时失去与卫星连接（或接收噪声信号）的情况并不少见，尤其是在拥有诸多高层建筑的城市中。类似地，使用过度利用的网络（例如，利用具有重传功能的TCP/IP协议）传输数据的传感器可能无法按时传递其测量结果，从而在消息到达时提供错误的信息。不过，由于瞬时故障的持续时间较短，因此不应将其视为对系统的安全威胁。

相反地，永久故障是传感器缺陷，它们会持续较长时间，并可能严重影响系统的运行。例如，传感器可能遭受物理损坏，从而在其测量值中引入永久性偏差。在这种情况下，除非可以在软件中纠正故障，否则系统将从完全丢弃此传感器中受益。

根据攻击者的目标，对传感器测量值的攻击可能表现为瞬时故障或永久故障。对攻击者而言，每种都有其优点和缺点。使传感器表现为瞬时故障可能阻止发现攻击者，但也会限制其能力，而类似于永久故障这样的持久攻击可能更强大，但可能被快速检测到。

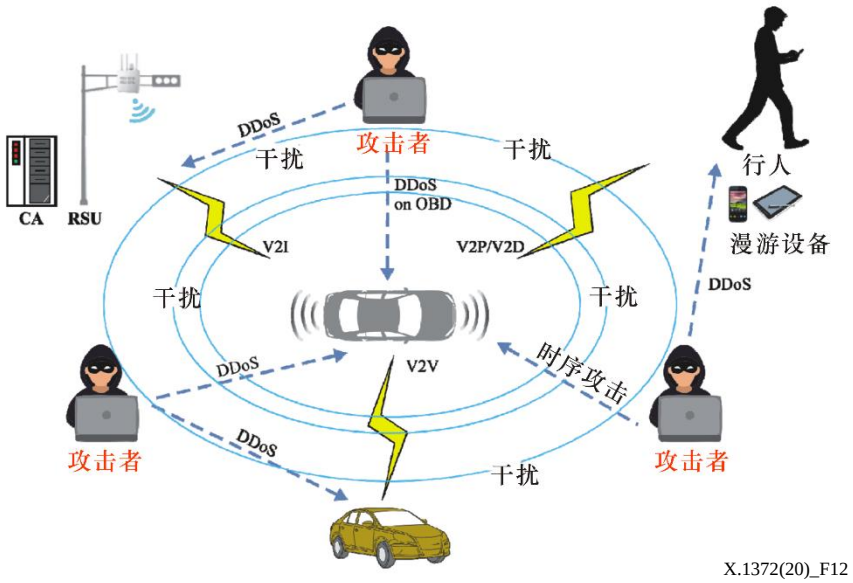


图12 – 对可用性的威胁

7.4 对不可否认性的威胁

图 13 具体说明本节描述的对不可否认性的威胁。

– 操纵认证数据库：

攻击者可操纵CA中的化名数据库，然后攻击者可修改长期证书与短期化名证书之间的关系。

– 未经授权地访问证书：

攻击者可未经授权地访问私钥和证书。如果私钥被暴露，则无法提供车辆、RSU和漫游设备的不可否认性。

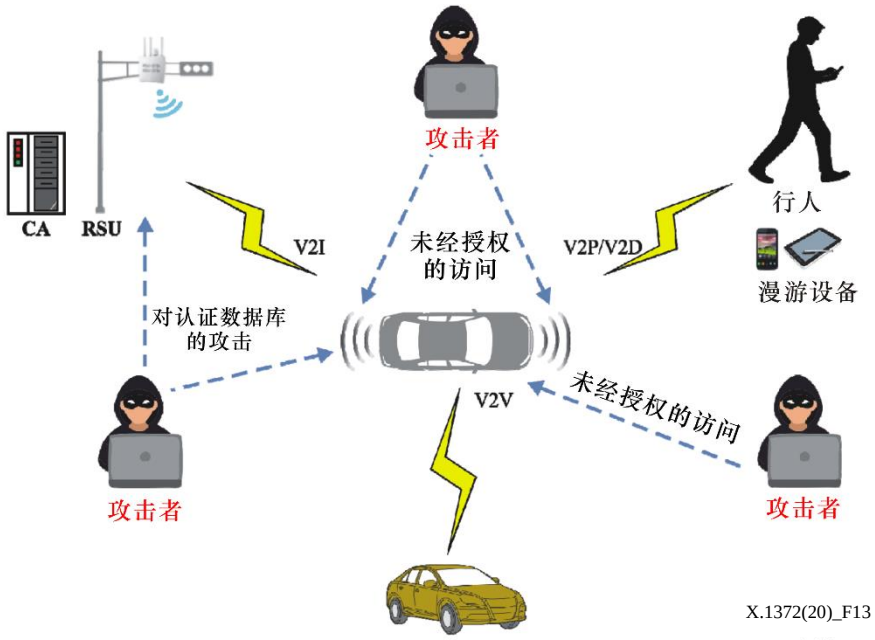


图13 – 对不可否认性的威胁

7.5 对真实性的威胁

图 14 具体说明本节描述的对真实性的威胁。

– 路由表和LDM修改攻击：

攻击者可欺骗车辆的GPS信息并修改其原始地理空间信息。

– 模仿攻击：

攻击者可通过窃取另一个实体的ID信息来伪装成另一个实体，而后，攻击者可接收通常发送给另一个实体的消息，也可发送看上去像通常由另一个实体生成的消息。例如，如果另一个实体是一辆紧急车辆，则攻击者可以向其他周围车辆发送消息，例如，“我是紧急车辆，请让路。”

攻击者还可代表一辆无辜车辆发送一个错误的故障信号，而后，CA可以吊销该无辜车辆。

– 女巫攻击：

当一辆车使用多个车辆ID模拟多辆车时，可能会发生女巫攻击。

– 化名分析攻击：

攻击者可分析车辆ID与化名之间的关系，以找到用于同一辆车的多个化名。

– 操纵认证数据库：

攻击者可操纵CA中的化名数据库，而后，攻击者可修改长期证书与短期化名证书之间的关系。

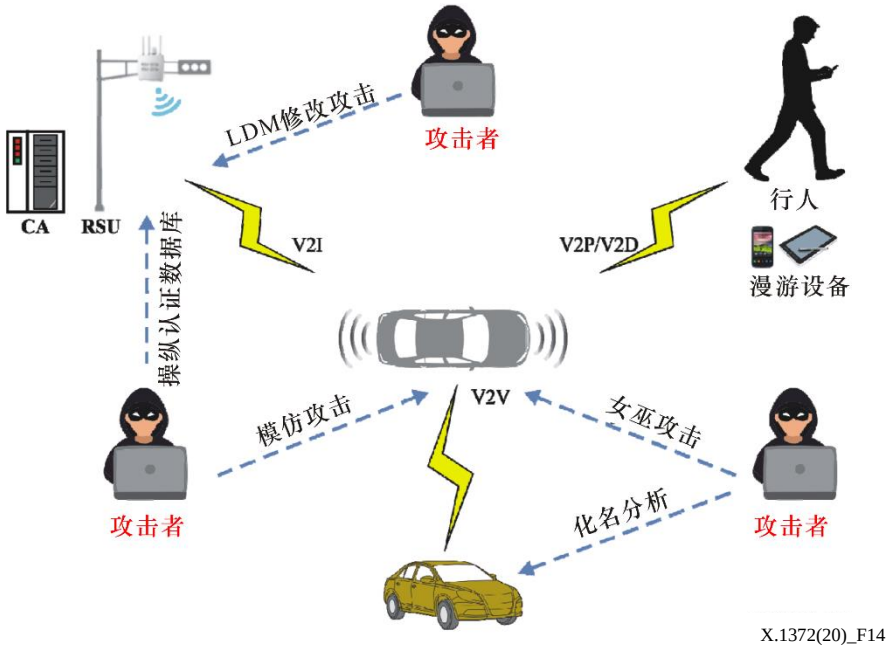


图14 – 对真实性的威胁

7.6 对可核查性的威胁

图 15 具体说明本节描述的对可核查性的威胁。

– 未经授权地复制漫游设备：

例如，由于某些特定的服务，如车辆诊断，一个授权的漫游设备可以访问车辆中的中央通信单元。不过，如果其授权被恶意设备复制（例如，如果经授权设备的登录账户已被另一个恶意设备使用即会出现这种情况），则该恶意设备可以访问通信单元。车辆内的中央通信单元可由一个未经授权的漫游设备所操纵。

– 未经授权地复制车辆和RSU：

攻击者获得（成功复制）车辆和RSU的ID后，原来的车辆和RSU将失去其可核查性。

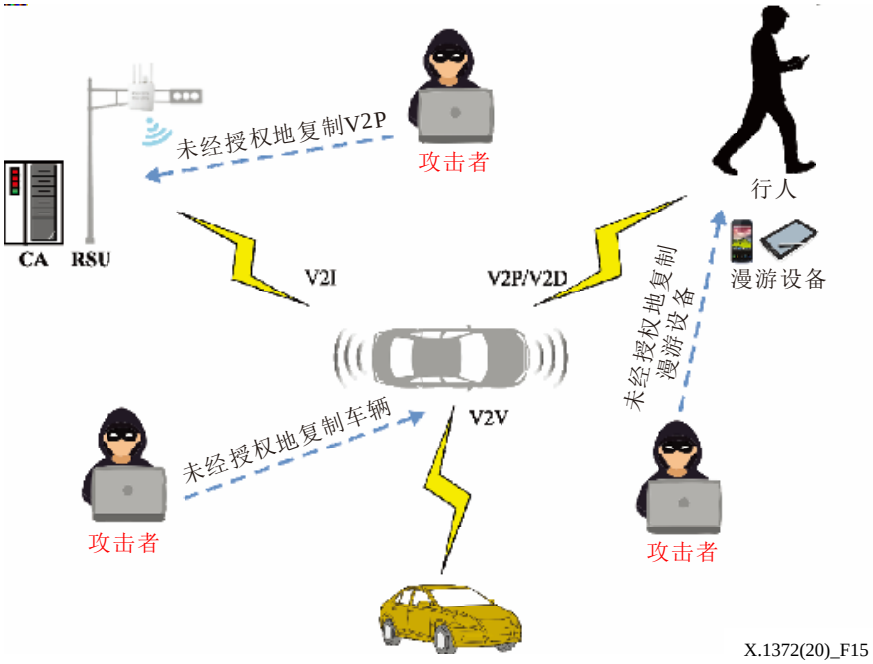


图15 – 对可核查性的威胁

7.7 对授权的威胁

图 16 具体说明本节描述的对授权的威胁。

– 未经授权地访问车辆中的安全敏感信息：

如果没有授权控制，则恶意用户或应用程序可以未经授权地控制车辆。例如，不应授权通过车辆中扬声器播放音乐的应用程序来访问安全敏感信息，例如车辆的速度和制动器的当前状态。

未经授权的攻击者还可操纵、擦除和重写安全敏感的车辆数据，包括车辆参数，例如紧急情况下的制动器和安全气囊阈值以及系统日志。

对于电动汽车，未经授权的攻击者可操纵汽车充电功能的配置参数。

– 未经授权地访问使用漫游设备的车辆中的某些功能：

定义连接到车辆的漫游设备的访问控制功能至关重要。漫游设备通常用于车辆中的音频、视频和导航工具。它还在多媒体主机上显示漫游设备的内容。未经授权的功能（例如使用该漫游设备与车辆中的中央网关进行通信）可能会对安全性造成严重的有害影响。

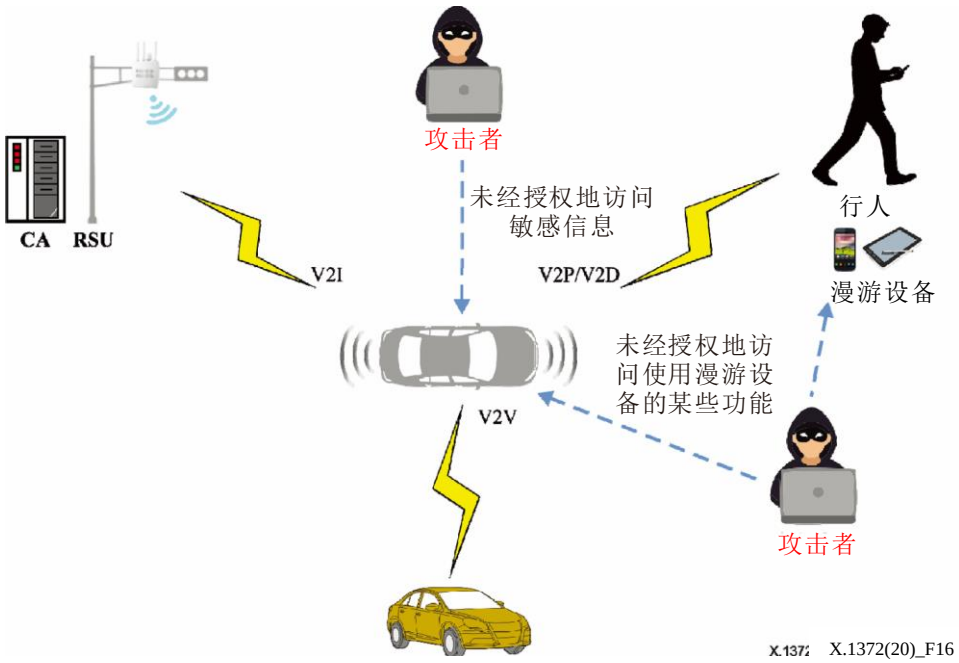


图16 – 对授权的威胁

8 安全要求

本节描述 V2X 通信的安全要求。第 8.1 至 8.7 节描述 V2X 通信中的安全要求，第 8.8 节提供有关这些要求的更多细节。

8.1 机密性

未经授权的实体应该不可能在车辆与车辆之间、车辆与基础设施之间、车辆与漫游设备之间以及车辆与行人之间披露消息。

未经授权的实体应该不可能通过通信消息内的个人可识别信息（PII）（例如特定人员的位置或行车路线）来分析人员的身份。

8.2 完整性

应该保护发送至车辆、RSU 或漫游设备或从其发送的消息，防止未经授权的修改和删除。

8.3 可用性

实体应该有可能以适当的延迟来发送和接收消息。例如，在车辆到达事故点之前，应该将前向碰撞告警消息发送到驶近的车辆。如果由于干扰攻击而无法将告警消息传递到驶近的车辆，则 V2V/V2I 安全应用程序可能是无效的。

实体应该有可能实时处理所交换的信息，因此它需要实现低开销和轻量级的加密算法。

8.4 不可否认性

实体应该不可能否认它已发送一条消息。可以使用 V2X 通信系统中的数字签名来实现此要求。

8.5 真实性

V2V/V2I 通信环境中诸如 OBU 和 RSU 之类的实体应该能够证明其是一个合法 ID 的授权拥有者。该要求称为实体验证。在车辆与漫游设备之间也需要它。

在组通信的情况下，车辆不需要证明其 ID。车辆应该证明它是该组的一个真实成员。该要求称为属性验证。

8.6 可核查性

实体应该可能通过检查 OBU 或车辆传感器的数据来检测和/或防止其不当行为。

例如，OBU 可以针对先前接收的消息，来检查所接收消息中的某些信息，以判断其运动学合理性。如果当前消息中的位置数据显示车辆的动态行为中存在不可能发生的变化，则可能是其他实体的不当行为。因此，可过滤或忽略该信息。

8.7 授权

定义不同实体的访问控制和授权至关重要。应强制执行特定规则，以访问或拒绝特定实体访问和/或使用某些功能或数据。

8.8 V2X安全要求的适用性

表 1 列出第 8.1 至 8.7 节中描述的安全要求以及这些要求在各种形式 V2X 通信方面的适用性。

表1 – V2X通信的安全要求

	V2V 告警传播	**V2V 排队通信**	**V2V 信标**	**V2I 告警**	**V2V/V2I 信息交换**	**V2D 通信**	**V2P 通信**
机密性（通用）	-	O	-	-	O	O	O
机密性（PII）	O	O	O	▲	O	O	O
完整性	O	O	O	O	O	O	O
可用性	O	O	O	O	O	▲	O
不可否认性	O	O	O	O	O	O	O
真实性	O	▲	O	O	O	O	O
可核查性	O	O	O	O	O	O	O
授权	-	O	-	-	O	O	-

O：要求，-：不要求，▲：部分要求

在 V2V 告警传播情况下，由于从一辆车到另一辆车的交换消息包含已公开的信息（例如前方交通事故或紧急车辆驶近），因此不需要强制保密。在 V2V 告警传播情况下，所传播消息不包含任何与授权有关的信息。

在 V2V 排队通信场景中，部分需要对车辆进行验证，这意味着不一定需要对组中的每辆车进行身份验证。实体验证是指一个实体向参与通信的另一个实体保证身份的过程。不过，在 V2V 排队场景中，每辆车都不需要对该组进行确切的实体验证。在这种情况下，只要足以证明每辆车都是该组的一个成员即可。换句话说，不保证车辆的身份，仅保证车辆是该组的一个成员。这种验证可被称为属性验证。该场景中的消息还具有授权信息，例如队长或队员。

在 V2V 信标场景中，应保护广播信息，防止未经授权的修改和删除。不过，如果该消息不包含车辆的识别信息，则不需要对消息进行加密。此外，V2V 信标场景不需要授权，因为广播的信息将不会用于控制目的。

在 V2I 告警场景中，车辆与 RSU 等基础设施之间的信息通常是公共共享的交通信息。这就是为什么在 V2I 告警环境中不需要机密性的原因。在 V2I 告警情况下，部分需要 PII 保护的标记意味着车辆需要 PII 保护，但 RSU 不需要 PII 保护。如果驾驶者链接到车辆，则应该保护车辆的当前位置和行驶历史。不过，由于 RSU 与人没有联系，因此 RSU 没有 PII。

在 V2D 通信场景中，漫游设备用于车辆中。当漫游设备与车辆进行通信时，可用性不会像 V2V 通信场景那样产生影响，因为在实际环境中，车辆中的设备数量实际上少于道路上的车辆数量。

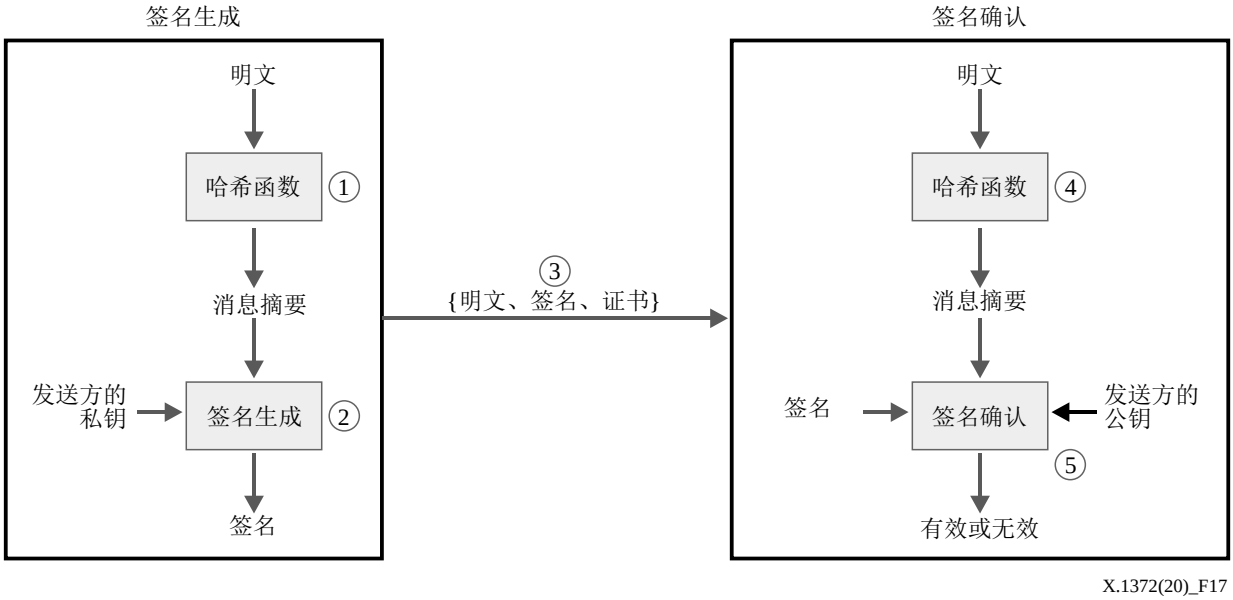
在 V2P 通信场景中，行人或 VRU 中的漫游设备不能具有需要车辆授权的任何功能。

9 安全V2X通信的实施方案

本节提供 V2X 通信的可能实施方案，以实现安全性要求，例如机密性、完整性、可用性等，这些要求在第 8 节中进行了描述。简要概述了适用于车载通信环境的基本密码算法，而后介绍了如何在 V2X 通信场景（如紧急告警和排队）中使用它们。

9.1 用于实体认证和消息保密的加密技术

V2X 实体验证功能可以使用数字签名算法来实现。可以使用对称和公共密钥密码算法来实现消息机密性功能。本建议书提供有关实现这些功能的例子。与实体验证和消息机密性功能相关的机制和参数的调整与选择取决于部署策略。



X.1372(20)_F17

图17 – 签名生成和确认

数字签名算法包括签名生成过程和签名确认过程，如图 17 所示。签名者使用该生成过程在数据上生成数字签名。确认者使用确认过程来确认签名的真实性。每个签名者都有一个公钥和私钥。如图 17 所示，私钥在签名生成过程中使用。签名者的公钥在签名确认过程中使用。

签名生成和确认的整个过程如下所述：

– 步骤1：使用哈希函数（例如安全哈希算法-256（SHA-256）），在明文消息上计算得到消息摘要。例如，在协议版本、报头、有效负载和报尾长度上计算得到摘要；
– 步骤2：使用发送方的私钥生成消息摘要的签名；
– 步骤3：将明文、签名和发送方的证书传送给接收方；
– 步骤4：接收方使用从发送方收到的明文计算得到消息摘要；
– 步骤5：接收方使用步骤4中的消息摘要、收到的签名以及发送方的公钥计算得到确认值。如果确认值与签名中的值相同，则接收到的签名有效。如果确认值与收到的签名中的值不同，则签名无效。

椭圆曲线数字签名算法（ECDSA）可以用作 V2X 通信中的数字签名算法。

加密算法用于支持 V2X 消息的机密性。诸如椭圆曲线综合加密方案（ECIES）之类的非对称加密算法用于为诸如高级加密标准（AES）之类的对称密钥算法传输密钥。ECIES 的加密过程如图 18 所述。在图 18 中，ECIES 使用以下功能：

– 密钥协商（KA）：两个实体用于生成一个共享秘密的函数；
– 密钥导出函数（KDF）：从密钥材料和一些可选参数中产生一组密钥的机制；
– 加密：对称密钥加密算法；
– 消息验证码（MAC）：MAC生成算法。

在图 18 中，使用以下记法：

– ***u***：发送方的私钥
– ***U***：发送方的公钥
– ***v***：接收方的私钥
– ***V***：接收方的公钥

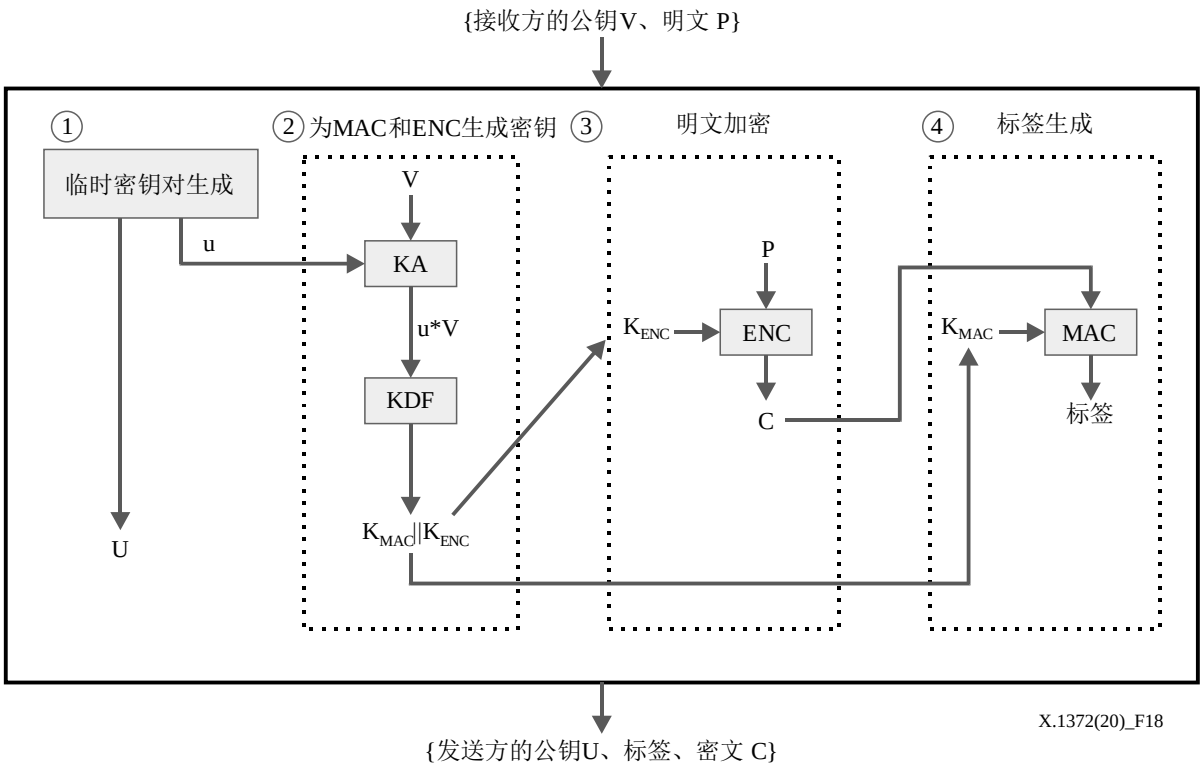


图18 – ECIES加密程序

如图 18 所示，加密过程的输入是接收方的公钥 ***V*** 和明文 ***P***。加密过程的输出是发送方的公钥 ***U***、标签和密文 ***C***。消息加密过程包括以下步骤：

– 步骤1：临时密钥对生成：

发送方生成私钥***u***和公钥***U***。建议为每个加密操作重新生成公钥***U***；

– 步骤2：为MAC和ENC生成密钥：

密钥协商函数（KA）通过发送方的临时私钥***u***和接收方的公钥***V***生成一个共享秘密。基于SHA-256的密钥导出函数（KDF）将采用该共享秘密来生成消息验证码（MAC）密钥（K_{MAC}）和加密密钥（K_{ENC}）串；

– 步骤3：对明文进行加密：

利用对称加密算法，使用K_{ENC}对明文***P***进行加密；

ECIES用于加密对称密钥，以使用高级加密标准-带有密码块链接消息认证码的计数器模式（AES-CCM）加密V2X消息。因此，明文实际上是AES-CCM的加密密钥；

– 步骤4：生成标签：

具有SHA-256的MAC函数生成密文的标签，它是AES-CCM的对称密钥，以支持消息的完整性。

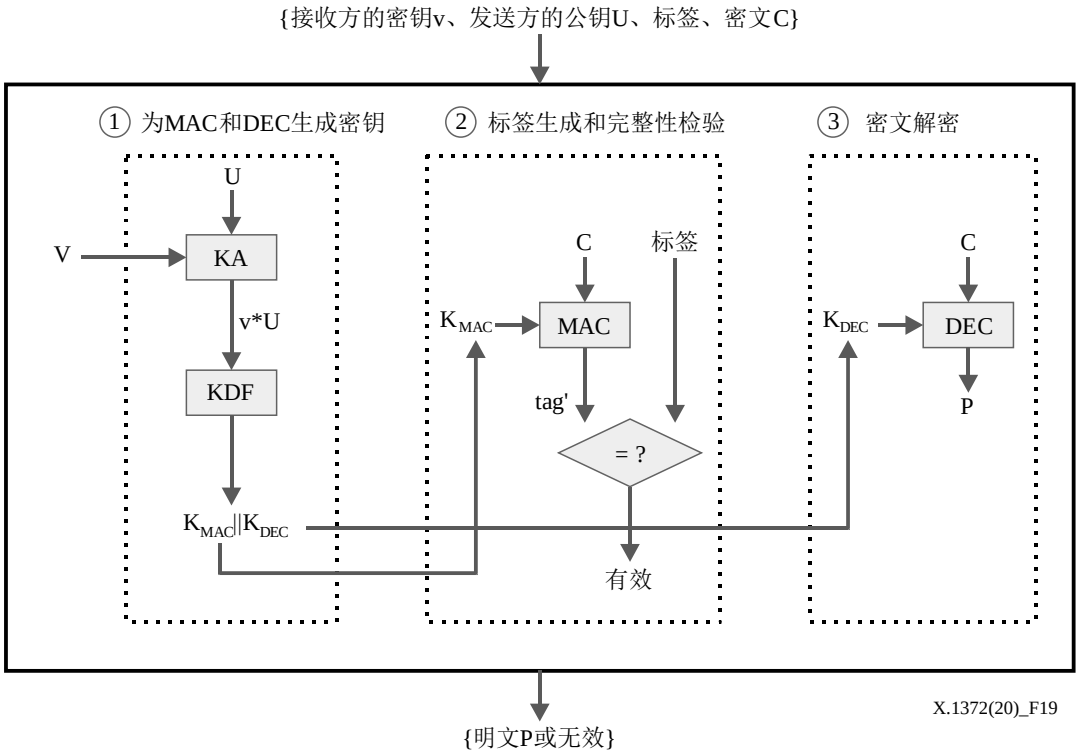


图19 – ECIES解密程序

ECIES 的解密过程在图 19 中予以描述。如图 19 所示，解密过程的输入是接收方的私钥 ***v***、发送方的公钥 ***U***、标签和密文 ***C***。解密过程的输出是明文 ***P*** 或消息完整性测试结果。图 19 中的 DEC 表示对称密钥算法的解密过程。消息解密过程包括以下步骤：

– 步骤1：为MAC和DEC生成密钥：

密钥协商函数（KA）由发送方的临时公钥***U***和接收方的私钥***v***生成一个共享秘密。基于SHA-256的密钥导出函数（KDF）将采用该共享秘密来生成消息验证码（MAC）密钥K_{MAC}和解密密钥K_{DEC}串。注意，在对称密钥算法中，K_{ENC}和K_{DEC}是相同的值；

– 步骤2：生成标签和完整性检验：

MAC函数利用K_{MAC}生成所收到密文***C***的标签。将计算得到的标签与收到的标签进行比较。如果值不相同，则因消息完整性检验失败而丢弃收到的消息；

– 步骤3：解密密文：

使用对称加密算法，利用K_{DEC}对密文***C***进行解密。

ECIES用于加密对称密钥，以使用 AES-CCM 加密 V2X 消息。因此，明文实际上是 AES-CCM 的加密密钥。

9.2 用于紧急道路安全告警的消息机密性

紧急告警的一个通用用例如图 20 所示。制动 ECU 通过其中央通信单元（CCU）向车辆的 V2X 通信单元发送消息。V2X 通信单元中的相应 ITS 应用程序从制动 ECU 接收消息，并生成 V2X 告警消息。生成的消息被发送到网络和传输层。该消息应由安全层签名或加密。而后，物理层将签名或加密过的消息发送到无线通信信道。使用无线通信信道，将消息发送到接收方。在接收方，安全层对消息进行确认或解密，并最终传递到上层，即相应的 ITS 应用程序。相应的 ITS 应用程序可利用人机接口设备更新 LDM 或向驾驶者发出告警，并可向制动 ECU 发送控制消息以降低车辆的速度。

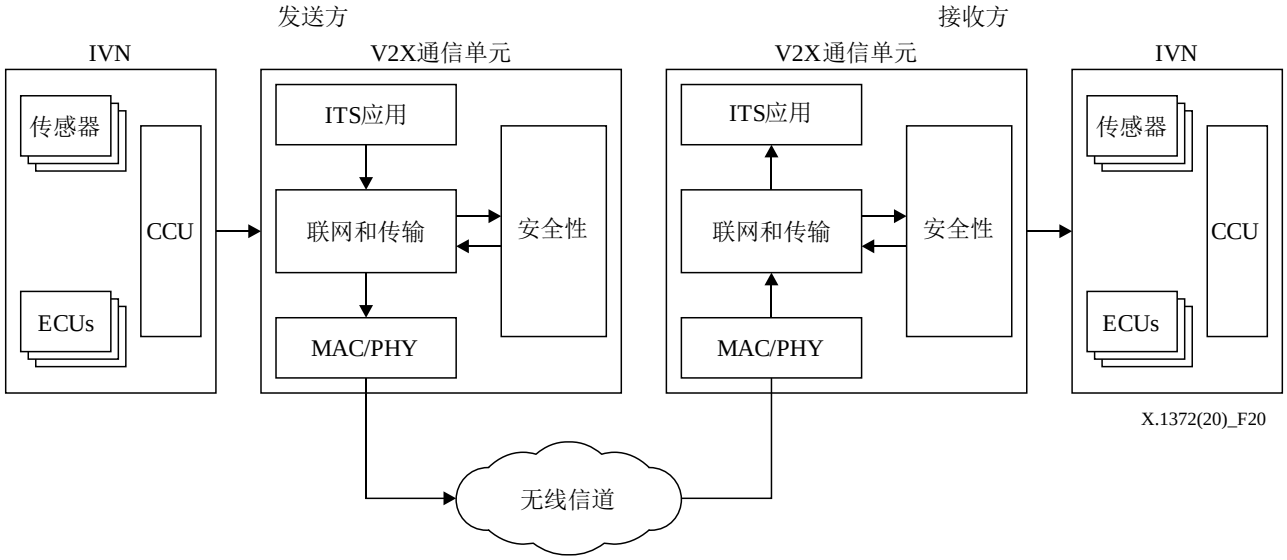


图20 – 紧急告警程序

9.3 用于车辆排队的实体认证

排队是将驾驶模式从个人驾驶改为基于队列驾驶的一种有效方法。通常，基于队列的驾驶涉及一组具有共同兴趣的车辆，其中一辆车跟随另一辆车并与前一辆车保持很小的、几乎恒定的距离，从而形成如图 21 所示的队列。在队列方面有三个主要过程：队列合并、队列合作/保持和队列拆分。

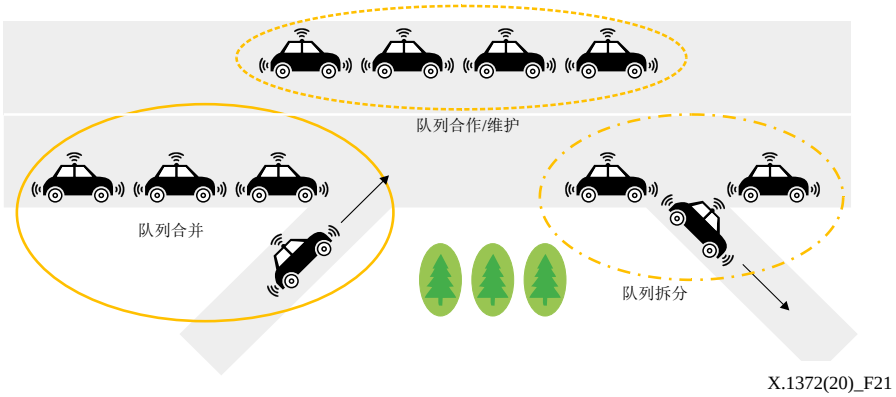


图21 – 排队用例

– 队列合并：不是队列成员的车辆将移动并合并到前方道路交叉口处的队列；

– 队列合作/保持：同一队列中的车辆需要相互通信和合作，以维护队列并完成诸如为优先级较高的车辆腾出道路、根据路线规划调整其位置、穿越交通路口和车道切换等任务；

– 队列拆分：车辆将从其队列拆分到前方道路交叉口处的另一条车道上。

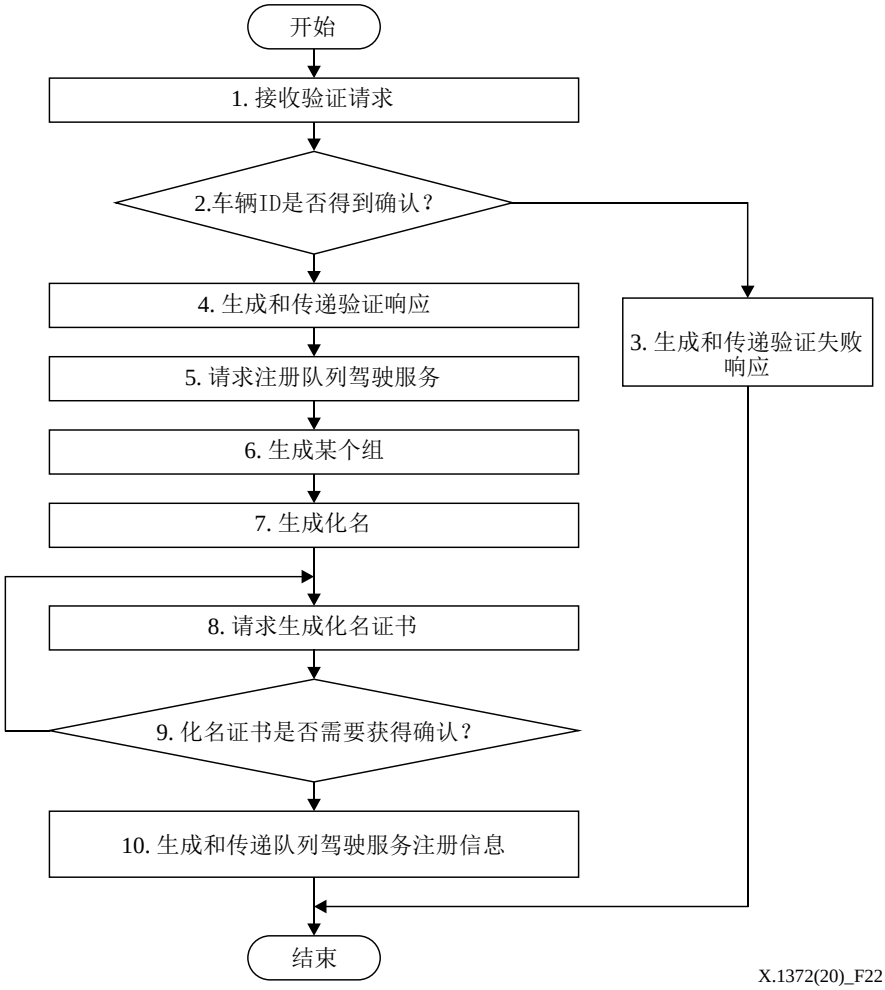


图22 – 队列注册程序

图 22 显示有关队列驾驶服务的验证示例。参照图 22，如果在步骤 1 的服务执行模式中从车辆接收到一个有关注册组驾驶服务的验证请求，即车辆验证请求，则在步骤 2 中应使用例如公钥密码系统的数字签名算法来确认车辆的 ID。在此，车辆的验证请求可以以以下方式来执行，即向组驾驶服务系统发送利用车辆私钥签名的消息。作为步骤 2 中的确认结果，如果确定车辆的 ID 是无效的，则如步骤 3 所示，组驾驶服务系统生成与其对应的验证失败响应，并将该响应发送给车辆。

作为步骤 2 中确认的结果，如果确定车辆的 ID 是有效的，则如步骤 4 所示，组驾驶服务系统生成车辆的验证响应，并将该响应发送给车辆。

之后，当接收到验证响应即实现对车辆的验证时，在用户输入并选择组驾驶注册信息（包括组驾驶资格、起始地、目的地、估计的出发时间、估计的到达时间和期望的休息地）后，车辆如步骤 5 所示将组驾驶注册信息发送给组驾驶服务系统，从而请求注册组驾驶服务。

随后，如果从车辆输入组驾驶服务注册请求（包括组驾驶注册信息），则组驾驶服务系统利用组驾驶注册信息（例如相同的目的地、相同的起始地、相同的估计到达时间等）生成一个特定组，然后如步骤 6 所示在组信息中存储/注册有关该特定组的信息。

在此，该特定组可以包括至少一个组长，即车辆领导者，以及至少一个成员，即车辆成员。此后，如步骤 7 所示，组驾驶服务系统为该特定组中的每辆车指派一个化名，生成证书请求消息，用于请求为指派给该特定组中每辆车的化名生成一个化名证书，并如步骤 8 所示将证书请求消息发送给验证中心。

在步骤 9 中组驾驶服务系统监视是否从验证中心获得了化名证书。作为监测结果，如果确保获得了化名证书，则组驾驶服务系统将化名证书存储在组信息数据库中。化名证书可以是验证中心的数字签名消息。通过化名证书有可能保证化名的合理性。化名是由组驾驶服务系统指派给每辆车的一个公开密钥。

可以为每辆车指派多个化名。由于化名不具有与每辆车的 ID 相关联的信息，因此不暴露参与组驾驶的车辆的 ID，从而有可能保护参与组驾驶的每辆车的 PII。

如果收到通知，则在步骤 10 中，组驾驶服务系统生成有关特定组的组驾驶服务注册信息，将其存储在组信息数据库中，并将其发送给特定组中的每辆车。在此，组驾驶服务注册信息可包括组 ID、指派给每辆车的化名、有关化名的化名证书等。注册了组驾驶服务的特定组中的每辆车（即车辆的用户），可使用从组驾驶服务提供的组驾驶服务注册信息，通过在特定组的车辆之间进行通信，来完成组驾驶。

9.4 车载PKI

促进和管理数字证书的公开密钥基础设施（PKI）对在车载通信环境中的参与者之间建立信任而言是必要的。车载 PKI 在若干方面有别于传统的 PKI。最重要的方面是使用化名来保护与车主位置有关的车辆位置。与传统的 PKI 相比，证书的数量巨大。因此，车载 PKI 的主要目的是提供用于请求证书和处理吊销的有效方法。

附录 II 更详细地描述了车载 PKI 的参考模型。

附录I

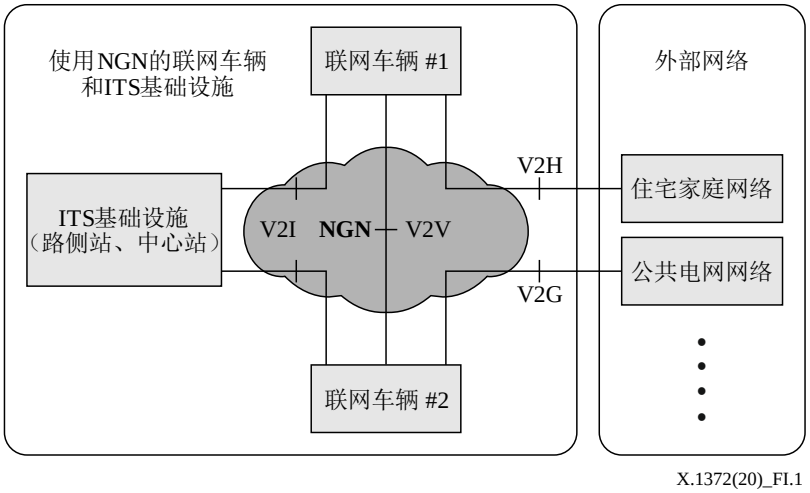
车载通信参考模型

（此附录不构成本建议书不可分割的组成部分。）

I.1 ITU-T利用NGN的联网车辆服务与应用的框架

[b-ITU-T Y.2281]中描述了下一代网络（NGN）环境中的联网车辆服务和应用程序框架。在车辆到基础设施（V2I）、车辆到车辆（V2V）和车辆到家庭（V2H）通信方面，车辆是利用网络功能的重要部件之一。在这种情况下，联网车辆可以与下一代网络（NGN）合作，以支持更高级的服务和应用程序，例如道路安全应用程序、与道路交通相关的应用程序、多媒体服务以及这些服务基于位置的实现。

[b-ITU-T Y.2281]确定 NGN 与联网车辆之间的关系以及考虑使用 NGN 支持联网车辆服务和应用程序之必要性的要求。此外，还描述了具备 NGN 功能的联网车辆和智能交通系统（ITS）基础设施的框架结构，以支持与联网车辆协调的 NGN 的通信功能。

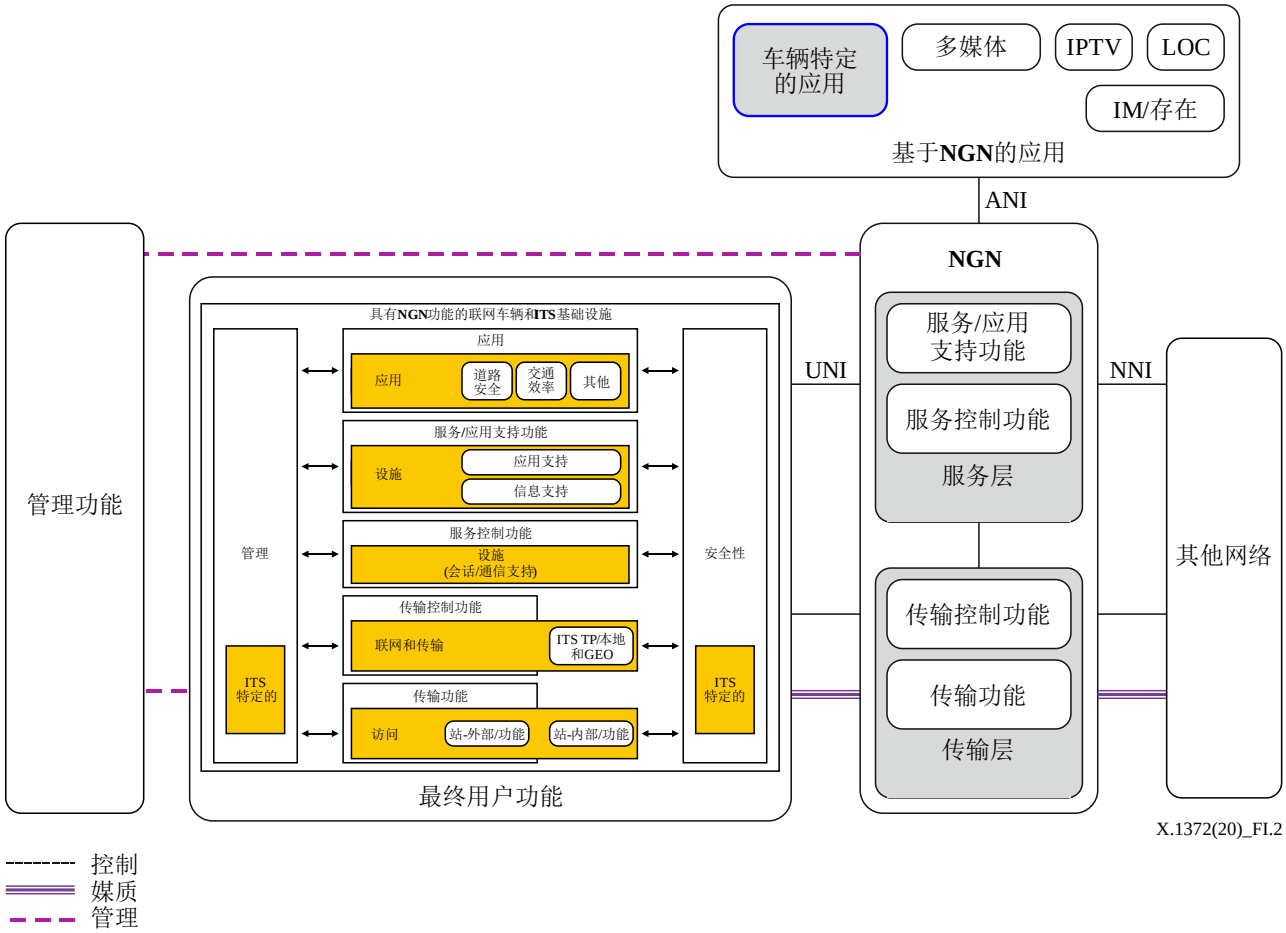


注 – 本图源自 [b-ITU-T Y.2281]。

图I.1 – 联网车辆和ITS基础设施的整体配置模型

图 I.1 显示了 ITU-T Y.2281 的配置模型，并显示了联网车辆如何与 ITS 基础设施以及包括住宅家庭网络和公共电网网络（使用 NGN 进行电力传输）的外部网络相关联。与其他 ITS 标准相比，[b-ITU-T Y.2281]专注于在 ITS 环境中使用 NGN。[b-ITU-T Y.2281]确定了在 ITS 环境中 NGN 的用法，以尽可能减少对等 ITS 通信与公共网络之间的互操作性问题。这些互操作性功能对利用各种多媒体服务支持服务质量（QoS）、移动性和安全性而言至关重要。

图 I.2 显示了与 NGN 合作的具有 NGN 功能的联网车辆和 ITS 基础设施的总体架构。NGN 由“最终用户功能”“服务层”“传输层”“管理层”和“基于 NGN 的应用程序”组成。考虑到 NGN，具有 NGN 功能的联网车辆和 ITS 基础设施的功能均置于最终用户功能上。[b-ITU-T Y.2281]描述了如何通过 NGN 支持诸如紧急呼叫之类的特定于车辆的 NGN 应用程序。



注 – 本图源自 [b-ITU-T Y.2281]。

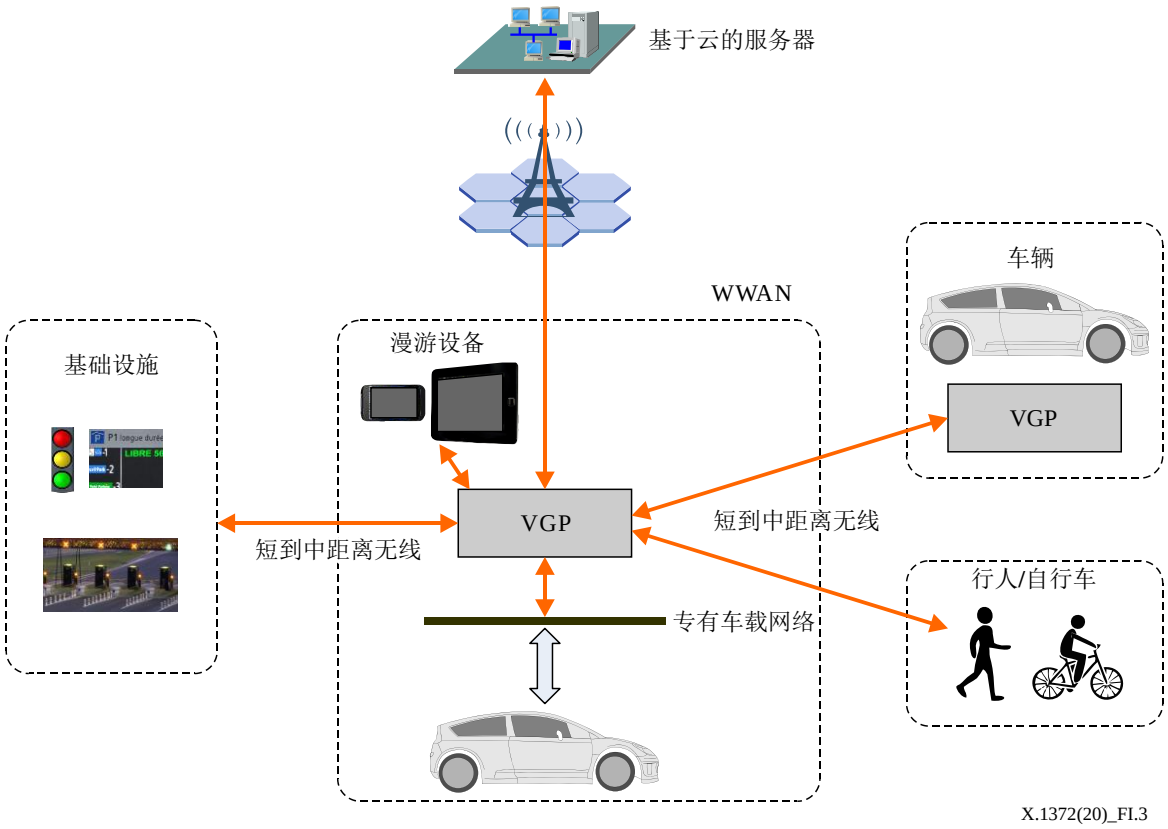
图I.2 – 与NGN合作的、具有NGN功能的联网车辆和ITS基础设施的体系结构概述

[b-ITU-T Y.2281]关于安全性的考虑参见 [b-ITU-T Y.2201]。依据连接到联网车辆的网络，需要考虑安全性。不过，[b-ITU-T Y.2281]仅规定了 NGN 对安全性的考虑，安全性要求的其他情况超出了[b-ITU-T Y.2281]的讨论范围。

使用 NGN 的联网车辆服务和应用程序的 ITU-T 框架专注于使 NGN 适应车辆环境。[b-ITU-T Y.2281]没有规定车载环境的安全性方面要求。[b-IEEE WAVE]中描述的 IEEE 车辆环境中的无线接入（WAVE）体系结构专注于 5.9 GHz 无线电接口，因为它没有明确包括与另一个网络进行通信的应用程序。[b-ETSI EN 302 665]中描述的 ETSI ITS 体系结构指的是“应用程序”层，它是用于通信的一个协议栈。考虑到“访问”层包括 IEEE 802.x、3G 蜂窝和蓝牙，ETSI ITS 体系结构旨在支持多个网络协议栈。

I.2 ITU-T车载网关平台的体系结构与功能实体

ITU-T 第 16 研究组负责研究车辆网关平台（VGP）的体系结构和功能实体。车辆网关平台的体系结构、功能体系结构框架和功能实体在[b-ITU-T H.550]中予以描述。VGP 的术语在[b-ITU-T F.749.1]中予以定义。VGP 是作为一个开放平台运行的车辆中信息通信技术软硬件集，以提供综合的运行时环境来提供车辆网关的通信服务。VGP 还可以提供更高层的通信服务，例如通过驾驶者-车辆访问服务与驾驶者进行交互等。专门用于车辆操作的子系统不被视为 VGP 的一部分。

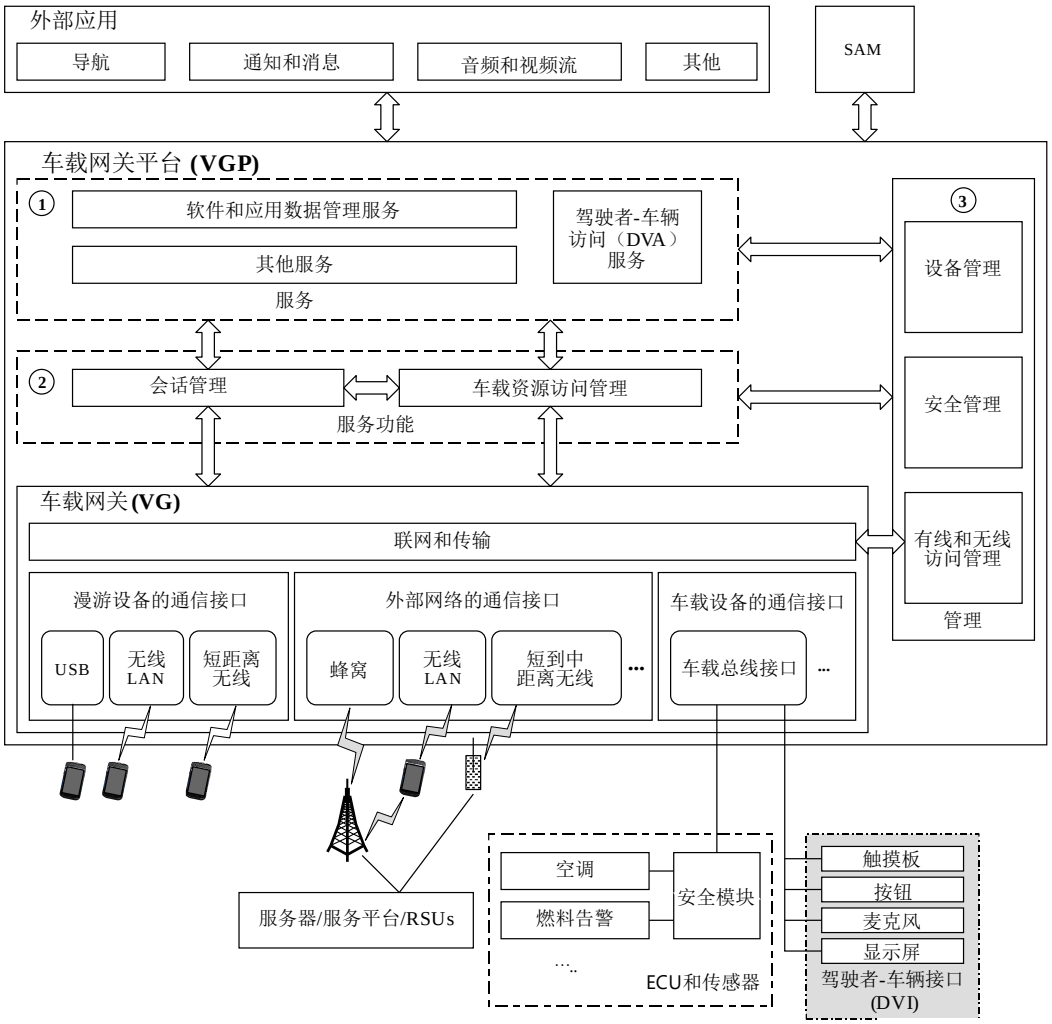


注 – 本图源自[b-ITU-T H.550]。

图I.3 – VGP在ITS参考模型中的位置

图 I.3 显示了智能交通系统（ITS）参考模型中的 VGP 定位：有六种主要情况，即车辆到车辆、车辆到基础设施、车辆到基于云的服务器、车辆到漫游设备、车辆到行人/自行车以及与车载网络进行交互的场景。

– 车辆到车辆（V2V）场景主要描述车辆与车辆相互通信的安全性和自动驾驶场景；
– 车辆到基础设施（V2I）场景主要描述安全性、电子收费系统（ETC）和交通信息交换场景，当中车辆与路侧基础设施进行通信；
– 车辆到基于云的服务器场景主要描述紧急呼叫和远程信息处理场景，当中车辆与基于云的服务进行通信；
– 车辆到漫游设备场景主要描述电信和远程用户界面（UI）场景，当中车辆连接到漫游设备；
– 车辆到行人/自行车场景主要描述安全告警场景，当中车辆与行人/自行车携带的设备进行通信；
– 与车载网络进行交互的场景主要描述车辆诊断、远程数据收集和车辆远程控制场景，当中VGP与专有车载网络进行通信。



注 – 本图源自[b-ITU-T H.550]。

图I.4 – VGP的高层体系结构

图 I.4 显示了 VGP 的高层体系结构。VGP 服务包括软件和应用程序数据管理服务、驾驶者-车辆访问服务以及其他服务（见图 I.4 中的方框（1））。服务功能包括会话管理和车载资源访问管理（见图 I.4 中的方框（2））。管理包括设备管理、安全管理以及有线和无线访问管理（见图 I.4 中的框（3））。服务支持诸如导航和信息娱乐之类的外部应用程序，以完成会话建立、数据格式转换和特定处理等。

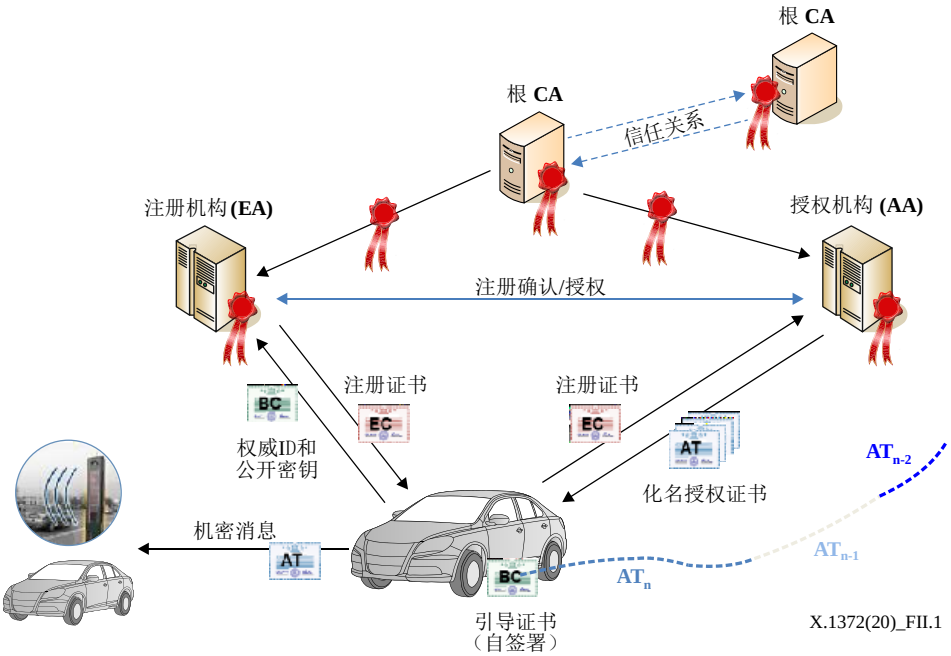
VGP 的安全性方面问题在[b-ITU-T H.550]中描述为管理层的一部分。[b-ITU-T H.550]第 8.4.1 节 – 安全管理 – 包含安全功能的一般描述。它由访问层的安全性管理（包括传输层和网络层）以及服务/应用程序的安全性管理组成。

附录II

车载PKI参考模型

（此附录不构成本建议书不可分割的组成部分。）

当前的 ITS 通信安全功能包括消息身份验证，这会对车辆和驾驶者的隐私产生影响。在欧洲层面，欧洲电信标准协会（ETSI）已定义了一种基于公共密钥基础设施使用的消息身份验证机制作为车载 PKI，如图 II.1 所示。



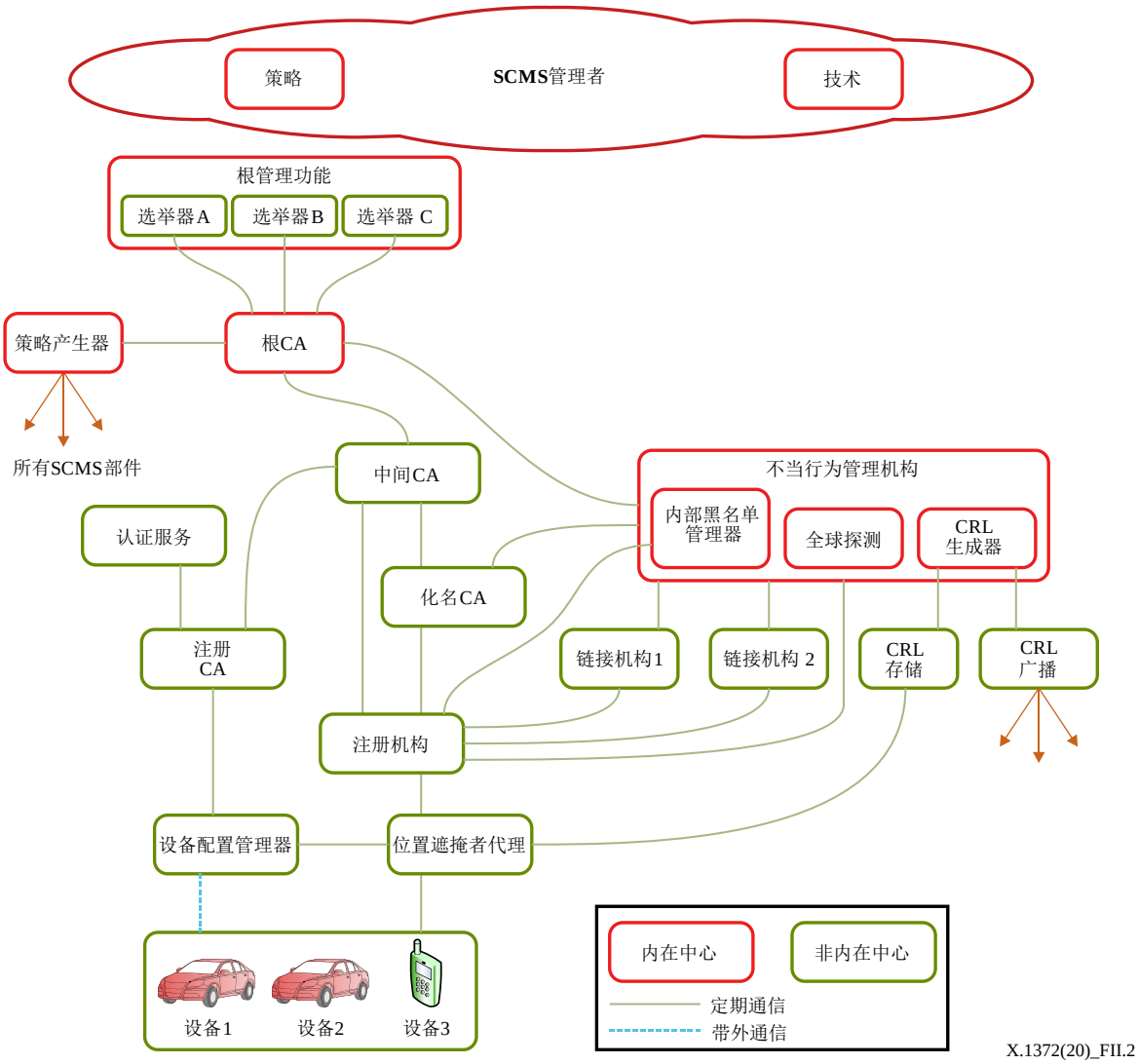
注 – 源自 [b-ETSI TS 102 940]。

图II.1 – ETSI中的车载PKI（来源：[b-ETSI TS 102 940]）

根证书颁发机构（RCA）是证书信任链的起点，它签署其他颁发机构，如授权机构（AA）和注册机构（EA）等的证书，并生成和维护证书吊销清单（CRL）、已吊销机构清单。在运行环境中，RCA 由一个可以确保较高和稳定置信度并充分联合的参与者（例如一个国家或一组国家）进行管理。EA 是提供注册证书（EC）并验证授权单（AT）请求的机构。AA 是向 ITS 站提供 AT 的受信任的第三方。AA 不知道 ITS 站的身份，依靠 EA 检查 ITS 站是否被授权拥有 AT。AT 请求包含 ITS 站注册所在的 EA 的身份。

本体系结构旨在为 ITS 站提供隐私保护并避免跟踪；EA 知道 ITS 站的身份，但不知道其使用的化名证书（AT），而 AA 知道 ITS 站的化名证书，但不知道其身份。ITS 站向 EA 注册并获得 EC。EC 用于向 AA 请求化名身份（AT）；当 ITS 站请求 AT 时，它将在请求消息中发送利用 EC 和 EA 身份加密的身份。AA 接收化名请求，读取 EA 标识符并检查 EA 接入点以验证 AT 请求。EA 检查 ITS 站 EC 并验证（或不验证）请求。如果请求得到验证，则 AA 生成 AT，并将其发送给 ITS 站。

另一方面，防撞指标合作伙伴（CAMP 联盟）提出了一种用于保护 V2X 通信安全的安全证书管理系统（SCMS）（见 [b-SCMS]）。它基于有关 V2X 安全性的 PKI，目前正从研究阶段过渡到概念验证阶段。SCMS 支持引导、证书提供、不当行为报告和吊销。



注 – 源自 [b-SCMS]。

图II.2 – CAMP中的V-PKI体系结构

图 II.2 概述了 SCMS 的体系结构。不同的 SCMS 部件之间的关系表示为线，它表示每个向其他部件发送信息或证书的部件。

SCMS 的主要部件如下所述：

– 注册CA（ECA）：为设备颁发注册证书，并可用于请求不同地理区域、制造商或设备类型的化名证书；

– 中间CA（ICA）：是一个二级证书机构，用于防止根CA承受繁重的通信负载，且其证书由根CA颁发；

– 链接机构（LA）：生成预链接值以形成链接值，该链接值放入证书中以进行有效吊销。此外，拆分LA旨在防止LA的运营商链接属于某个特定设备的证书；

– 位置遮掩者代理（LOP）：更改源地址以隐藏请求设备的位置，并防止将网络地址链接到位置；

– 不当行为管理机构（MA）：接收并处理来自设备的不当行为报告，以确定潜在的不当行为或故障。此外，它将吊销设备的证书并将其放入CRL。MA还启动将证书标识符链接到相应注册证书并将其放入RA内部黑名单的过程；
– 策略产生器（PG）：维护RA全局策略文件的更新。全局策略文件包含全局配置信息，以及全局证书链文件，该文件包含SCMS的所有信任链；
– 化名CA（PCA）：向设备颁发短期化名、标识和应用程序证书。每个PCA都限于某个特定的地理区域、特定的制造商或设备类型；
– 注册机构（RA）：验证并处理来自设备的请求，并确保已吊销的设备不能够颁发新的化名证书。此外，RA在给定时间段内不会向设备颁发多套证书。此外，RA在将化名证书签名请求发送给PCA或将信息转发给MA之前，会对请求或报告进行“洗牌”；
– 根证书机构（RCA）：是SCMS中证书链的根和顶，为ICA、PG和MA颁发证书。

参考书目

[b-ITU-T F.749.1] ITU-T F.749.1 建议书（2015 年），车载网关的功能要求。

[b-ITU-T H.550] ITU-T H.550 建议书（2017 年），车载网关平台的体系结构与功能实体。

[b-ITU-T X.509] ITU-T X.509 建议书（2019 年），信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架。

[b-ITU-T X.641] ITU-T X.641 建议书（1997 年），信息技术 – 服务质量：框架。

[b-ITU-T X.800] ITU-T X.800 建议书（1991 年），CCITT 应用的开放系统互连（OSI）安全体系结构。

[b-ITU-T X.813] ITU-T X.813 建议书（1996 年），信息技术 – 开放系统互连 – 开放系统中的安全框架：不可否认性框架。

[b-ITU-T X.1252] ITU-T X.1252 建议书（2010 年），身份管理基准术语和定义。

[b-ITU-T X.1371] ITU-T X.1371 建议书（2019年）联网汽车的安全威胁。

[b-ITU-T Y.2201] ITU-T Y.2201 建议书（2009 年），ITU-T 下一代网络（NGN）的要求和性能。

[b-ITU-T Y.2281] ITU-T Y.2281 建议书（2011 年），利用下一代网络（NGN）的联网车辆服务与应用的框架。

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture.<https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*.<https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] IEEE Std. 1609.2 (2016), *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*.

[b-ISO 13185-1] ISO/TR 13185-1:2012, *Intelligent transport systems – Vehicle interface for provisioning and support of ITS services – Part 1: General information and use case definition*.

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Website). <https://www.oversee-project.com/>

[b-RITA] United States Department of Transportation, FHWA-JPO-11-130 (2011), An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues. <https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications. 5 (VSC5) Consortium, *Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, 04*. May. 2016.

<https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] United Nations Secretary of the Informal document GRVA-01-17, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA.*

[b-US DOT] United States Department of Transportation, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] United States Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] United States Senator for Massachusetts, Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦