国　际　电　信　联　盟

ITU-T X.1376

(01/2021)

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

利用大数据针对与联网车辆安全相关的不当行为开展检测的机制

ITU-T X.1376建议书

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

ITU-T X.1376建议书

利用大数据针对与联网车辆安全相关的不当行为开展检测的机制

摘要

ITU-T X.1376建议书描述一种针对联网车辆的安全相关不当行为检测机制，以帮助利益攸关方利用汽车数据来提高车辆安全性。

随着车辆连通性的增加，由于复杂技术的发展，漏洞的数量也在增加。这些漏洞给联网车辆带来了更多威胁。对大量汽车数据进行分析对于评估联网车辆的安全性非常有用。

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.1376	2021-01-07	17	11.1002/1000/14448

关键词

联网车辆；不当行为检测。

* 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ID，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已收到实施本建议书可能需要的受专利/软件版权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，因此大力提倡他们通过ITU-T网址查询相应的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1376建议书

利用大数据针对与联网车辆安全相关的不当行为开展检测的机制

1 范围

本建议书描述一种针对联网车辆的安全相关不当行为检测机制。该机制包括以下步骤：

a) 数据采集。指定可用于不当行为检测的、从不同来源获取的数据和信息类型，包括汽车、基础设施、原始设备制造商（OEM）和供应商。数据采集方法和程序不属于本建议书的范围。

b) 检测。分析采集的数据以检测不当行为。

本建议书适用于联网车辆，目的是方便设计人员和安全解决方案提供商检测不当行为。通知的使用不在本建议书的范围内。

2 参考文献

下列ITU-T建议书和其他参考文献包含的条款，通过本文的引用构成本建议书的条款。在出版时，所指示的版本有效。所有建议书和其他参考文献均可能进行修订；因此，鼓励本建议书的用户研究应用建议书最新版本和下面列出的其他参考文献的可能性。定期发布当前有效的ITU-T建议书清单。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

无。

3 定义

3.1 它处定义的术语

无。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.1.1 不当行为：提供虚假或误导性数据的行为，以妨碍其他服务接受者或超出其授权范围的方式运作。不当行为可能来自车辆系统的内部或外部组件。

注1 – 基于[b-ISO/TR 17427-4]。

注2 – 不当行为包括有意或无意的错误消息类型或频次、无效登录和未经授权的访问，或不正确的签名或加密消息等可疑行为。

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：

ADAS 先进驾驶辅助系统

ABS 防滑制动系统

AEB 自动紧急制动

API 应用程序编程接口
CAN 控制器局域网
GNSS 全球导航卫星系统
ITS 智能交通系统
IP 互联网协议
LiDAR 光探测和测距
MCU 微控制器单元
OEM 原始设备制造商
TCU 远程信息处理控制单元
URL 统一资源定位符

5 惯例

无。

6 不当行为检测机制模式

图1提供联网车辆的不当行为检测机制模式。该机制包括数据采集和检测两个步骤，由两个系统实现。

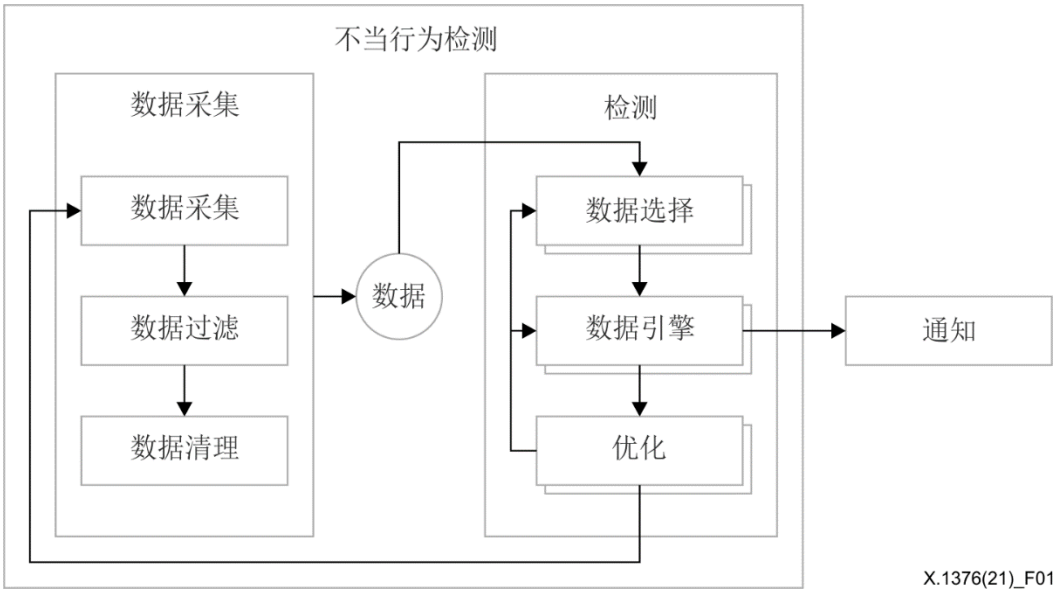


图 1 – 不当行为检测机制模式

由于数据采集方法和程序不在本建议书的范围内，因此图1中的数据采集系统（例如数据过滤和数据清理）只是不当行为检测实际实施的供参考示例。

来自采集系统的数据被发送至检测系统，且采集到的数据根据第7节中描述的类型进行处理。

数据采集系统包括以下模块：

a) 数据采集：采集不同渠道，如服务提供商、车身系统和传感器，的检测数据；

b) 数据过滤：根据数据分类过滤采集到的数据；

c) 数据清理：对采集到的数据进行重复数据删除和降噪处理。

检测系统包括以下模块：

a) 数据选择：基于不同的不当行为检测方法选择数据集，然后将其发送至检测引擎；

b) 检测引擎：根据检测方法检测不当行为，然后酌情将决策结果发送至优化和通知单元；

c) 优化：使用来自检测引擎的检测结果改进数据选择、检测引擎和数据采集。

通知是一个模块，将检测引擎的输出信息发送给利益攸关方。该模块不属于本建议书的范围。

7 数据采集

数据采集通常包括数据捕获、数据清理和数据过滤。由于数据采集方法和程序不在本建议书的范围内，因此本建议书仅规定检测程序中使用的数据类型。应使用适当的技术，如匿名化等，对所有个人敏感数据进行保护，但这不属于本建议书的范围。

根据从不同来源采集的数据和信息，本节规定不当行为检测机制中使用的数据类型，即状态数据、控制数据和智能数据（intelligence data），具体见表1。

表1 – 数据类型

类型	子类型	数据来源	数据示例
状态数据[a]	应用/服务数据	内容提供商或服务提供商	信息数据
		地图服务数据	导航、定位
		移动应用数据	应用相关数据
	车辆状态	安全系统	防滑刹车系统（ABS）、安全气囊、自动紧急刹车（AEB）、高级驾驶员辅助系统（ADAS）
		车身系统	门、窗、雨刷
		底盘系统	扭矩，拐角
		动力系统	速度、转速、节流阀、档位
	环境传感器	雷达	毫米波雷达
		光探测和测距（LiDAR）	点云
		超声传感器	距离
		摄像头	周围环境图像
		智能交通系统（ITS）传感器	路边设施标志
控制数据[b]	本地控制	车辆内控制器	开门、关门
	远程控制	自动化、远程信息处理	远程诊断
智能数据[c]	内部智能数据	安全性研究、测试结果	漏洞、缺陷、内部网络安全事件
	外部共享智能数据	客户、供应商、社区、会议/文献、网络	互联网协议（IP）地址、哈希值、统一资源定位符（URL）、域名、常见漏洞和暴露（CVE）等。

[a] 与智能交通系统中的车辆、应用、服务、传感器和其他设施的状态相关的数据和信息。

[b] 用于控制智能交通系统中车辆、应用、服务、传感器和其他设施的数据和信息。

[c] 从智能交通系统外部获得的与网络安全相关的数据和信息。假设数据源的完整性适当。

8 检测

检测模块主要由数据选择、检测引擎和优化部分组成。如图2所示，基于来自不同来源的数据和信息，检测引擎使用大数据分析识别不当行为。优化部分使用不当行为优化数据选择，检测引擎使不当行为检测更加准确和高效。

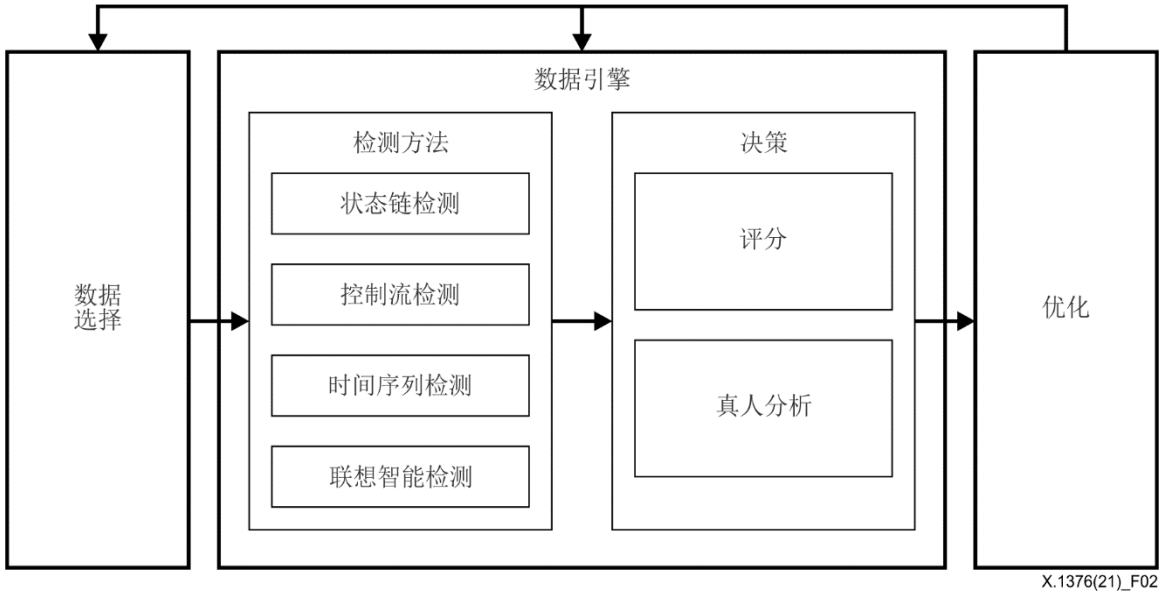


图 2 – 检测程序

8.1 数据选择

数据选择模块根据检测方法对数据的不同要求，按照检测引擎的要求将数据分为不同的数据集，见图3。数据选择模块的输入是来自采集系统的数据。

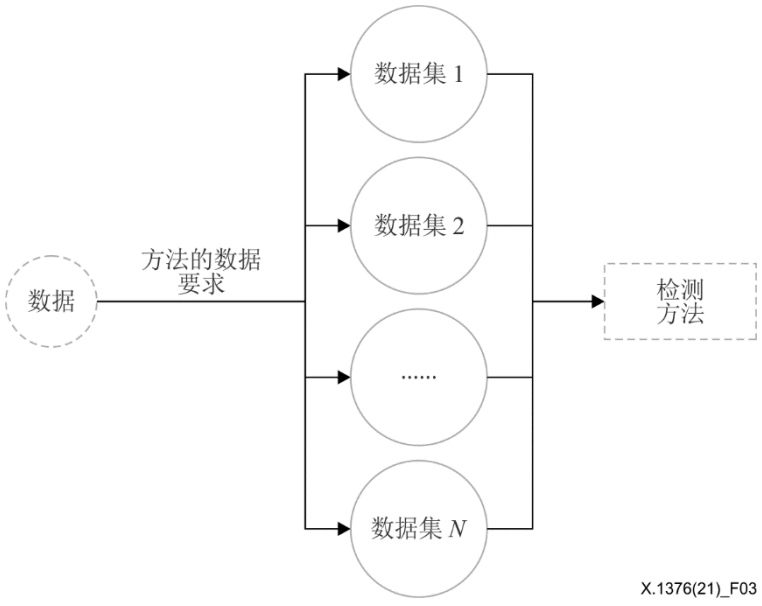


图 3 – 数据选择程序

8.2 检测引擎

检测引擎由两个子模块组成：检测方法和决策。当数据集进入检测方法子模块时，方法会将其转化为行为特征。然后，决策子模块基于行为特征做出决策。有三种不同类型的决策结果：阻止、可疑、允许。阻止意味着情况异常；可疑意味着无法确定数据是被拒绝还是安全的；允许意味着数据是安全的。

8.2.1 检测方法

检测方法子模块是一组不同的检测方法。基于第7节中分类的数据类型，设计了四种方法来使用这些数据检测不当行为。

8.2.1.1 状态链检测

状态链包含一系列相关联的状态数据。在状态链中，一个数据的改变会导致其他数据同时改变。

状态链的一些特点如下：

a) 节点：智能交通系统中与某一行为相关的服务或应用；

b) 流程：改变数据方向和路径的动作。

状态数据在智能交通系统中生成，可用这些数据创建语境。数据值也遵循一定的趋势，并在一定范围内波动。

本质上而言，状态链可分为线和分支两种模式。这两种模式如下：

1) 线模式：每个节点只有一个接收其信号的节点；

2) 分支模式：一个节点同时生成两个或多个状态数据，然后将其发送到不同的节点。

在状态链的线模式中，节点只有单向连接。见图4。

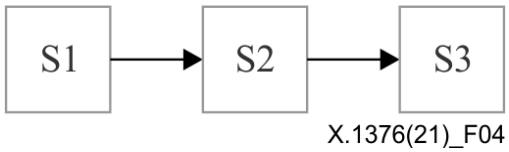


图 4 – 状态链的线模式

S：状态

在状态链的分支模式中，节点可以分为两个或多个相关的线模式。见图5。

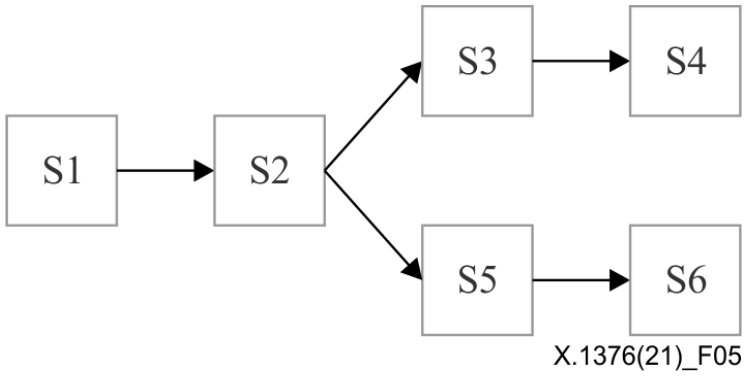


图 5 – 状态链的分支模式

因此，每个节点的特征包括：

i) 状态链中的语境；

ii) 每个节点的值和趋势。

获得来自状态链中节点的特征，然后将其发送到评分功能单元。

8.2.1.2 控制流检测

控制流包含一系列相关的控制数据。在控制流中，一个控制命令可由多个子控制命令组成，并将影响多个系统。

描述控制命令执行的控制流的一些特点如下：

a) 节点：智能交通系统中与某项行动相关的服务或应用；

b) 流程：一个动作所产生的数据变化的方向和路径。

当控制动作进行时，控制相关数据将通过控制相关节点并形成控制流。

智能交通系统中的每个控制节点都稳定而有规律地工作。当许多节点一起工作时，由于规定的周期、确定的消息类型和数量，所以控制流的行为也是稳定的。

本质上，控制流可分为线和分支两种模式，具体如下：

1) 线模式：每个节点只有一个接收其信号的节点：

2) 分支模式：一个节点同时生成两个或多个状态数据，然后将其发送到不同的节点。

在线模式控制流中，节点只有单向连接。见图6。

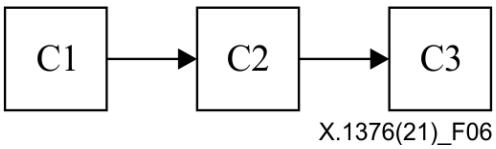


图 6 – 控制流的线模式

C：控制

在控制流的分支模式中，节点可以分为两个或多个相关的线模式。见图7。

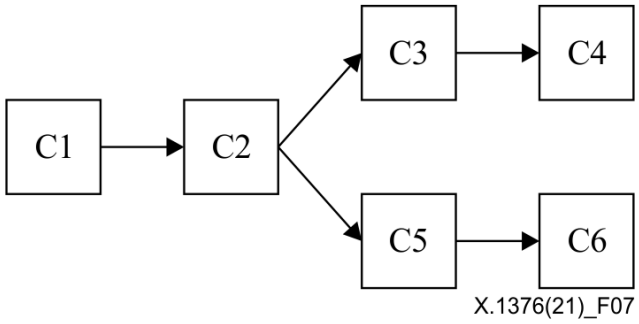


图 7 – 控制流的分支模式

8.2.1.3 时间序列检测

时间序列用于描述根据类型而变化的数据。只要数据符合类型，那么就可以使用时间序列检测。

序列数据的变化趋势有四种类型：

a) 趋势：数据随时间或自变量变化，表现出相对缓慢和长期的趋势，具有连续上升、下降或保持不变的相同性质，但变化幅度可能不相等；

b) 周期性：一个因素随着时间的推移逐渐显示出重复的特性，包括波峰和波谷；

c) 随机性：数据是随机变化的，但总体情况是可统计的；

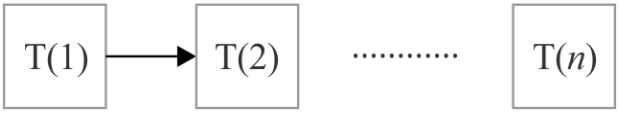
d) 叠加：实际变化是几个变化的叠加或组合。

时间序列行为的一些特点如下：

1) 节点：智能交通系统中与时间序列数据相关的服务或应用；

2) 流程：按时间顺序显示时间。

许多数据属于时间序列数据，例如控制器局域网（CAN）消息。可以用一种或多种类型的数据来建立数据模式，以发现不当行为。见图8。



X.1376(21)_F08

图 8 – 时间序列的线模式

T：时间

8.2.1.4 联想智能检测

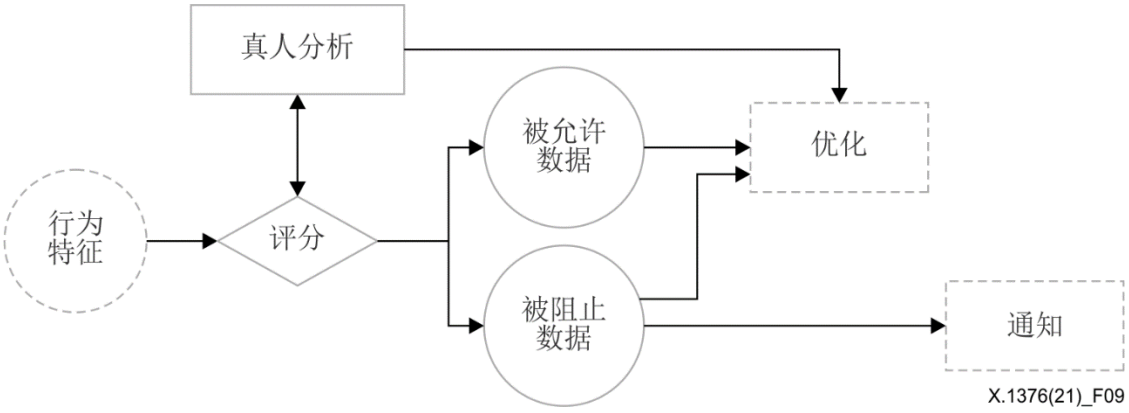
对于联想智能检测方法，可以直接或间接检测不当行为，因此，联想智能数据可以分为两类：直接和间接数据。

直接联想智能：可基于该智能直接检测不当行为，例如外部漏洞报告、内部网络安全研究和常见漏洞披露。

间接联想智能：基于这种智能不能直接检测不当行为，因为这种智能用于描述正常事件，例如，错误修复、新功能发布、软件更新和芯片更换。将间接联想智能与采集到的其他数据相结合，可以检测出不当行为。

8.2.2 决策

本节介绍图9所示的决策子模块程序。



X.1376(21)_F09

图 9 – 决策子模块中的程序

决策子模块用于确定检测方法的结果，包括两个功能：评分和真人分析。评分功能通过行为特征确定数据类型，然后对其进行评分。如果不当行为（如劫持或篡改攻击）发生，它就会偏离稳定性基线。如果分数不能达到允许或阻止的阈值，则被归类为可疑。然后，人工分析师将介入并帮助做出决定，直到分数达到被允许或被阻止数据的阈值。

8.3 优化

优化是一个反馈模块，它从检测引擎处接收数据，并使用这些数据来优化自身。见图10。

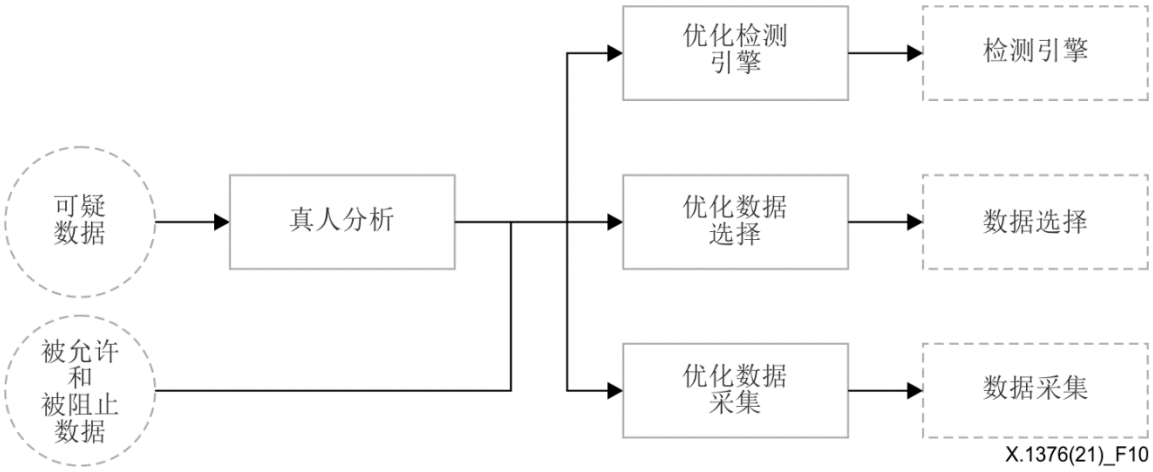


图 10 – 优化程序

8.3.1 优化检测引擎

特性是流程中每个被传输数据的关键值。在不当行为检测开始时，稳定性基线是由正常环境中的正常特征生成的。评分功能得到初始化。

检测引擎通过其输出进行优化。增加、修改或删除检测方法，以提高检测效率；评分功能也通过增加从真人分析中获得的新知识而得到优化。

8.3.2 优化数据选择

通过增加、修改或删除数据集来提高检测准确度。

8.3.3 优化数据采集

添加、修改或删除采集到的数据，以提高检测准确度。

附录一

不同检测方法的使用案例

（此附录并非本建议书不可分割的组成部分）

本附录提供如何按照第8.2.1节中的不同检测方法检测不当行为的使用案例。

I.1 状态链案例

这是第8.2.1.1段所述的状态链检测案例。

车辆配有一个通信模块，称为远程信息处理控制单元（TCU），用于访问互联网。TCU不是一直在运行，所以它在车辆发动机停止后会切换到低功率模式以节省功率。在进入低功率模式之前，它将车辆状态发送到车辆网关（后端服务），车辆网关将该状态同步到TCU状态缓存。然后，命令服务从TCU状态缓存中获取该状态。当用户向其车辆发送命令时，命令服务根据TCU状态做出反应。如果TCU处于低功率模式，则命令服务会向唤醒服务发送请求，然后唤醒TCU。图I.1显示正常的行为。表I.1显示这种正常行为所涉及的状态数据。

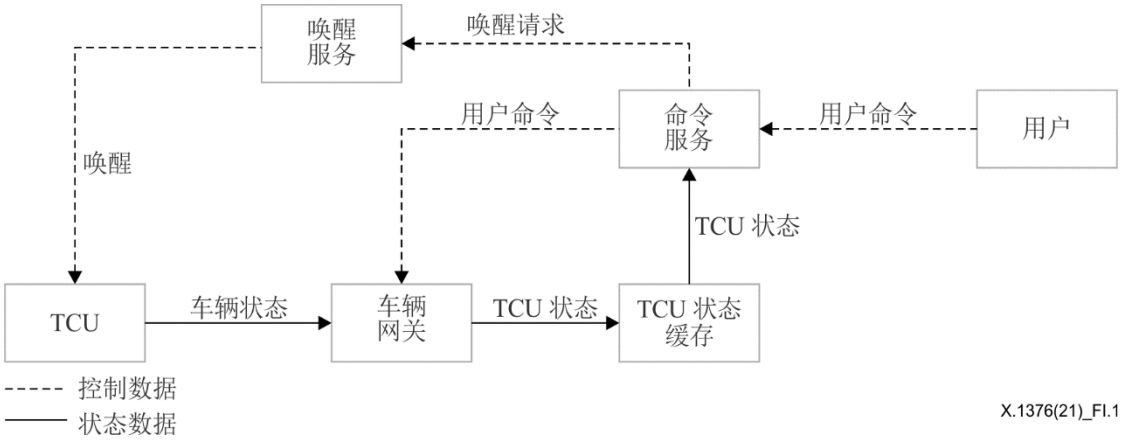


图 I.1 – 状态链的正常行为

当攻击者想弄清楚这个程序时，他们会尝试修改TCU状态，以查看命令服务表现出的不同行为。这时TCU状态缓存和车辆网关之间将会出现差异。

在这种情况下，状态链检测可通过比较车辆网关中的车辆状态和TCU状态缓存中的TCU状态来检测不当行为。如果其状态不同，则这即是一种不当行为。车辆行驶时，TCU不能处于低功率模式。

表 I.1 – 车辆驾驶状态数据

节点	数据
车辆网关	车辆状态
TCU状态缓存	TCU状态
命令服务	TCU状态

I.2 控制流案例

这是第8.2.1.2段的控制流检测案例。

当用户想远程控制车辆时，需要使用安装在用户智能手机上的应用程序来触发该功能。应用程序将生成操作日志，然后应用程序将向后端应用程序编程接口（API）服务发送请求，后者将在访问日志中记录这一请求。之后，API服务将预处理该请求，并将其转发至车辆端点，如TCU。TCU将调用带有收发信器的微控制器单元（(MCU)，并向相关执行器发送命令。最后，执行器将执行来自用户侧的控制命令。见图I.3。表I.2显示这种正常行为所涉及的控制数据。

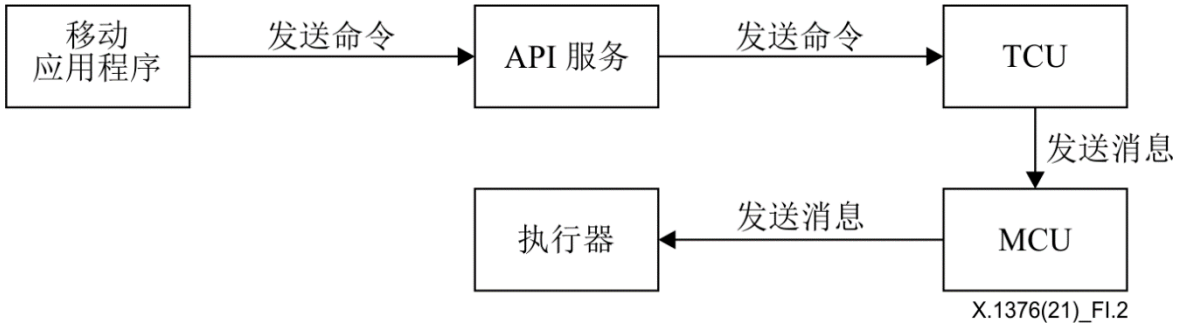


图 I.2 – 控制流的正常行为

在这种情况下，只有当API服务发出请求时，TCU才会向MCU发送消息。如果从异常路径调用MCU，则移动应用程序和API服务中不会有操作日志。之后将检测到不当行为。

表 I.2 – 远程信息处理控制数据

节点	数据
移动应用程序	操作日志
API服务	访问日志
TCU	已接收数据
MCU	调用日志
执行器	执行器日志

I.3 时间序列案例

这是第8.2.1.3段的时间序列检测案例。

在这种情况下，TCU定期向后端服务发送车辆的位置。见图I.3。

Latitude (°)	Interval (s)
39.9544	10.4015592431
39.9566	10.2439587253
39.9594	10.5735141799
39.9502	10.3234362303
39.9528	10.0973092011
39.9538	10.5066656864
39.9558	10.4945798327
39.9556	10.1209659368
39.9506	10.2163646279
39.9551	10.1042228459

图 I.3 – 位置的正常时间序列

如果全球导航卫星系统（GNSS）传感器处于欺骗干扰（spoofing）状态，位置信息和间隔将与此前数据有明显的差异。见图I.4。

Latitude (°)	Interval (s)
39.9503	10.4741553595
39.9595	10.2682504585
39.9597	10.2750387130
39.9568	10.4752930715
39.9520	10.6371744699
45.1525	5.4110037357
39.9597	5.5768263688
39.9508	10.4367481108
39.9550	10.0731090275
39.9529	10.5550728359
39.9518	10.5853553005
39.9554	10.1983262711

图 I.4 – 位置的不当行为时间序列

表I.3显示车辆中常见的时间序列数据。

表 I.3 – 自动传感器时间序列数据

节点	数据
后端服务	纬度、间隔

I.4 联想智能检测案例

第8.2.1.4段阐述了两种联想智能检测情况，因此此处提供两个使用案例，每种情况一个。

I.4.1 直接联想智能检测案例

基于直接联想智能检测不当行为是联网车辆中最简单的方法。所有形式的直接联想智能都直接指向不当行为，例如，IP地址、域名、URL、内部网络安全研究和外部漏洞报告。这些数据中的任何一个都包含检测不当行为的绝对特征。

表I.4显示智能交通系统中常见的直接联想智能。

表 I.4 – 直接联想智能检测数据

节点	数据
车载信息娱乐系统	IP地址 URL 域名
智能数据库	外部漏洞报告 内部网络安全研究

I.4.2 间接联想智能检测案例

间接联想智能不能独立用于检测不当行为，但可以与其他智能来源结合使用。在某些情况下，单个漏洞无法被利用，但攻击者可利用多个漏洞构建利用链来实现利用。例如，并不是每个供应商都修复漏洞以防止其被利用。当检测引擎收到关于链接（chaining）的新技术报告时，[b-CVE-2017-11906]和[b-CVE-2017-11907]可进行任意代码执行；可采集车载信息娱乐系统中的浏览器版本，以便与智能数据一起用于检测不当行为。

表I.5显示智能交通系统中常见的间接联想智能。

表 I.5 – 间接联想智能检测数据

节点	数据
智能数据库	车载信息娱乐系统 外部技术报告

参考书目

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Intelligent transport systems – Cooperative ITS – Part 4: Minimum system requirements and behaviour for core systems*.

[b-CVE-2017-11906] Common Vulnerabilities and Exposures, CVE-2017-11906 (2017). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906

[b-CVE-2017-11907] Common Vulnerabilities and Exposures, CVE-2017-11907 (2017). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Available [viewed 2021-02-21] at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907

ITU-T 系列建议书

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
2021年，日内瓦