蜂窝车联网中的物理层安全问题

Physical Layer Security Issues in C-V2X Communication

沈霞/SHEN Xia，周伟/ZHOU Wei，王志勤/WANG Zhiqin
（中国信息通信研究院，中国 北京 100191）
(China Academy of Information and Communications Technology, Beijing 100191, China)

DOI：10.12142/ZTETJ.202203014
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20220516.1519.006.html
网络出版日期：2022-05-17
收稿日期：2022-02-20

摘要：蜂窝车联网在驾驶环境中不仅对传输时延和可靠性有较高的要求，还对通信安全性有很高的要求。分析了蜂窝车联网物理层通信中的安全问题，包括边链路通信中物理层数据的恶意解析和基于终端自主资源分配模式的非正常信道占用问题。提出的专用单播通信标识和非正常信道占用的问题监测与识别方案，可使蜂窝车联网的物理层通信安全性得到有效提升。

关键词：蜂窝车联网；物理层安全；无线通信；边链路

Abstract: Cellular vehicle-to-everything (C-V2X) has stringent requirements not only on the wireless communication delay and reliability in the driving environment, but also on the communication security. The physical layer security issues in the C-V2X communication are analyzed, including malicious detecting of physical data and abnormal channel occupation using resource allocation method based on channel sensing. Solutions through allocating dedicated scrambling ID for unicast communication and abnormal channel occupation monitoring and identification scheme are put forward to deal with those problems, respectively, and the communication security of C-V2X would thus be effectively improved.

Keywords: C-V2X; physical layer security; wireless communication; sidelink

基于移动通信的蜂窝车联网（C-V2X）技术是面向车辆场景通信业务需求的关键技术，也是中国目前主要推广的车联网通信技术。该技术支持车与路边设施、车与车之间的通信。其中，路边设施可以是基站，也可以是终端。车和基站之间的通信类似于手机终端和基站之间的通信，即利用上行和下行通信进行信息交互。车和车之间以及车和终端模式下的路边设施之间的通信模式主要有两种：一种是基于基站调度的通信模式，另一种是基于终端自主资源分配的通信模式。对于前者，终端和终端的通信资源均由基站分配调度，源节点在向其他终端发送数据之前需要向基站发出资源分配请求；对于后者，终端在基站分配或者预配置的一个资源池上侦听信道，并选择空闲或者干扰较小的信道资源发送数据。相对来说，基站调度的通信模式可以避免终端间通信干扰和隐藏节点下的传输碰撞问题，但是会引入较大的传输时延；终端自主资源分配的通信模式可以让终端快速接入信道，但是会遇到信道拥塞、传输碰撞等问题。

C-V2X经历了4G长期演进车联网（LTE-V2X）和5G新空口车联网（NR-V2X）两个阶段，并且主要在终端和终端之间的通信边链路（SL）上开展设计。在4G LTE-V2X中，终端间的通信主要支持广播模式下的周期性业务；5G NR-V2X则在功能上做了进一步增强，支持广播、组播和单播模式下的周期和非周期性业务。其中，单播还支持终端间的信道测量反馈和传输混合自动重传请求（HARQ）反馈，以增强单播和组播的可靠性。5G NR-V2X同时支持多种子载波间隔和高低频通信，传输配置更加灵活。目前，诸如部分侦听、非连续接收（DRX）、终端间协作、中继等5G NR V2X标准正在制订当中。制订这些标准的目的是减少终端能耗，提升终端之间通信的可靠性，增强网络覆盖。此外，非授权频段、高频段、载波聚合等方面的增强后续也将受到关注。

C-V2X的安全问题目前已成为车联网产业化应用的一个焦点问题。中国在2021年9月8日正式启动了车联网身份认证和安全信任试点工作[1]，以便为车联网中的通信设备构建可信的“数字身份”认证和管理体系，避免非法设备的身份伪造和安全攻击。车联网安全主要包括终端与设施安全、网联通信安全、数据安全、应用服务安全等[2]。相应的安全技术标准已经制定，例如《YD/T 3594-2019 基于LTE的车联网通信安全技术要求》[3]等。针对C-V2X网联通信安全，人们搭建了LTE-V2X安全架构，制定了终端设备与核心网之间、终端与终端之间、终端与基站之间、基站与核心网之

基金项目：国家重点研发计划（2020YFB1807501）

间，以及核心网网元之间非接入层上的接口[3]和接入层中分组数据汇聚协议（PDCP）层之上的安全技术标准。这类标准主要通过传统加密认证的方式来构建安全可行的链接[4]。而接入层PDCP层之下，尤其是SL上的物理层安全问题则相对比较突出。在目前标准约定的方法中，物理层可根据应用层的指示随机更改该层通信所使用的层2-ID和设备IP地址[4]。然而，这种方法并不能避免物理层数据被窃取分析的问题。本文对C-V2X终端间通信的物理层安全问题展开深入分析，并针对问题提出相应的解决方案。

1 C-V2X物理层安全问题分析

C-V2X物理层安全问题主要包括两个方面：一是终端的物理层信息可以被恶意监听的终端接收并识别，二是信道被终端恶意长期占用导致其他终端无法正常接入信道。这两方面的安全问题在一定程度上均来源于现有技术的设计：现有终端解析物理层信息方案导致PDCP层以下的物理层信息被恶意监听，基于信道侦听的终端自主资源分配方式导致终端高优先级业务长期抢占信道。下面我们对现有技术下的具体物理层安全问题展开分析。

1.1 C-V2X物理层信息解析方案中的安全问题

对于C-V2X通信的边链路对应的物理边链路控制信道（PSSCH）和物理边链路共享信道（PSCCH），边链路通信以广播为主，并没有分配类似于蜂窝链路上终端专用的小区无线网络临时标识（C-RNTI）去加扰PSSCH和PSCCH。在4G LTE V2X中，具体的加扰方式[5]为：PSCCH采用以固定初值$c_{\text{init}}=510$初始化的加扰器生成的加扰序列进行加扰，PSSCH采用初值为$c_{\text{init}}=n_{\text{ID}}\cdot 2^{14}+n_{\text{ssf}}^{\text{PSSCH}}\cdot 2^{9}+510$初始化的加扰器生成的加扰序列进行加扰。其中，参数$n_{\text{ID}}=\sum_{i=0}^{L-1}p_i\cdot 2^{L-1-i}$，$p$和$L$分别为指示该PSSCH传输的控制信道PSCCH的循环冗余校验（CRC）序列的相关比特位取值和长度；参数$n_{\text{ssf}}^{\text{PSSCH}}$取值为$t_k^{\text{SL}} \bmod 10$，$t_k^{\text{SL}}$为PSSCH传输所在的子帧号。5G NR V2X中，虽然引入了单播和组播传输模式，但是PSCCH和PSSCH的加扰方式基本延用了LTE V2X的加扰机制。NR PSCCH采用以固定初值$c_{\text{init}}=1\,010$初始化的加扰器生成的加扰序列进行加扰；NR PSSCH采用初值为$c_{\text{init}}=2^{15}n_{ID}+1\,010$初始化的加扰器生成的加扰序列进行加扰，不再与PSSCH传输所在的子帧号绑定[6]。

LTE V2X终端检测PSSCH和PSCCH的基本流程为：在网络配置的PSCCH资源位置上采用盲检的方式检测PSCCH，在解扰PSCCH上承载的边链路控制信息（SCI）之后，进一步在SCI指示的PSSCH资源位置上接收检测PSSCH，并对PSSCH进行解扰解析。NR V2X引入了2阶SCI设计[7]，其中PSCCH承载1st SCI，PSSCH承载2nd SCI。2nd SCI的格式在1st SCI中指示。终端根据检测的1st SCI的指示，在PSSCH上先检测2nd SCI信息，再根据2nd SCI信息中指示的HARQ信息检测PSSCH中的数据部分。在引入单播和主播之后，NR V2X会在SCI信息中指示目的节点层1-ID信息。如果检测到SCI中的身份标识（ID）与自身ID信息匹配，接收终端则会进一步检测对应的PSSCH，否则不做进一步检测。

在解析出物理层PSSCH的数据部分之后，接收终端会将数据进一步传递给媒体接入控制（MAC）层，并识别MAC层的包头内容。MAC层包头中也包含ID信息，这些信息为源节点和目的节点层2-ID的部分信息。接收终端会进一步判断该ID信息所配置的源节点与目的节点的层2-ID信息是否匹配。如果匹配，接收终端会进一步将解析的MAC层数据上传给PDCP层，否则将丢弃数据。在不同传输模式下，SCI和MAC包头指示节点的ID信息会有所不同，具体如表1所示。

由上述PSSCH和PSCCH的加扰方式以及终端检测数据流程可知，物理层信道的解扰检测并未与源节点层2-ID、目的节点层2-ID以及组层2-ID实际绑定，终端仅通过接收的SCI和MAC包头中的ID信息来判断是否与自身的ID相匹

▼表1 C-V2X中物理层节点ID指示[8-9]

传输模式	SCI中指示ID（层1-ID）	MAC包头指示ID
广播（LTE-V2X）	无	源节点ID：源节点层2-ID 24位信息 目的节点ID：目的节点层2-ID 24位信息
组播（NR-V2X）	源节点ID：源节点层2-ID[1]低8位 目的节点ID：组节点层2-ID[2]低16位信息	源节点ID：源节点层2-ID高16位 目的节点ID：组节点层2-ID高8位信息
单播（NR-V2X）	源节点ID：源节点层2-ID低8位 目的节点ID：目的节点层2-ID低16位信息	源节点ID：源节点层2-ID高16位 目的节点ID：目的节点层2-ID高8位信息

注1：源节点层2-ID和目的节点层2-ID应用层业务相关，通过应用层ID与层2-ID的映射关系确定。
注2：组节点层2-ID为组播模式下接收组的ID信息，应用层提供V2X组标识以确定组节点层2-ID。
C-V2X：蜂窝车联网　ID：身份标识　LTE-V2X：长期演进车联网　MAC：媒体接入控制　NR-V2X：新空口车联网　SCI：边链路控制信息

配，进而选择是否将数据进一步传递给上层。一个非目的节点或者非组内成员的终端，也可直接将监听的单播或者组播的物理层数据（不管是否与自身设备的层2-ID匹配）传递给上层进行解析。一个恶意的节点可以在单播通信的连接建立过程中利用监听获取源节点层2-ID和目的节点层2-ID的信息，恶意占用信道资源向源节点和目的节点发送信息，干扰正常的单播通信，如图1所示。

1.2 C-V2X终端自主资源分配方案中的安全问题

LTE-V2X和NR-V2X都支持终端自主资源分配方案。该方案的基本设计思路为：源节点首先侦听信道占用情况，在一个资源选择窗$[n+T_1,n+T_2]$内基于信道侦听结果确定一个候选资源集，然后在候选资源集中选择传输资源。其中，n为资源选择触发时刻。候选资源集主要由源节点判断的未被占用的信道资源组成，或者由已被占用但是测量的参考信号接收功率（RSRP）低于设定阈值的信道资源组成。为了保证源节点有足够的候选资源可使用，并且每个信道资源上的业务量是平均化的，候选资源集中的资源数量应不低于资源选择窗中总资源数量的占比X。其中，X在LTE-V2X中固定为20%，在NR-V2X中则可配。在资源选择过程中，如果候选资源集的资源数量低于上述占比X，系统将会降低判定被占用资源的RSRP阈值，将更多的资源判定为候选资源，直到候选资源数量达到占比要求。在资源选择过程中，不论信道是否拥塞，发送数据的源节点都可以通过上述方法选择到资源以用于发送数据。尽管如此，源节点的发送参数配置仍然受到拥塞控制机制的限制。拥塞控制机制规定了不同优先级下不同信道拥塞状态的信道占比限制情况。如果源节点不同优先级传输选择占用的资源总量超过规定的信道占比限制，则需要丢弃低优先级的传输，以缓解信道拥塞，减少资源碰撞。

由此可见，拥塞控制机制在一定程度上保证了高优先级业务的传输。为了进一步保障高优先级业务的传输，NR-V2X引入了资源抢占机制[10]，即高优先级业务可以抢占低优先级业务占用的传输资源。在发送SCI指示占用的传输资源之后，源节点在利用传输资源发送数据之前会持续进行信道侦听。当侦听到有更高优先级业务抢占指示的传输资源时，且测量的RSRP高于阈值，源节点则判定资源被抢占，需要进行资源重选。因此，一般节点如果亟需接入信道而无合适的资源选择时，可以将被低优先级业务占用的信道资源作为候选资源。低优先级业务对应的源节点会通过信道侦听发现资源抢占，从而退避并进行资源重选，避免传输碰撞。

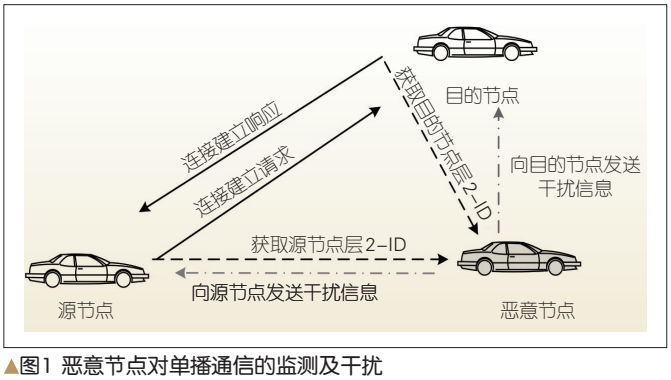
在终端自主资源选择的模式下，拥塞控制机制和资源抢占机制在保障高优先级业务传输的同时也引入了一定的安全问题。例如，当某个节点拥塞控制机制出现故障或者不使用该机制，同时该节点仍处于信道拥塞环境中并且需要大量业务进行传输时，信道拥塞的程度无疑会加重，传输干扰也会增加。此外，如果一个功能故障节点或者恶意节点将其传输业务设置为最高优先级，持续地发送数据占用或者抢占信道，则在NR-V2X场景下，低优先级业务的节点在移动到功能故障节点或者恶意节点附近时就无法接入信道，功能故障节点或者恶意节点的周围就形成一个通信盲区，如图2所示。这将带来一定的安全隐患。

2 C-V2X物理层安全方案设计

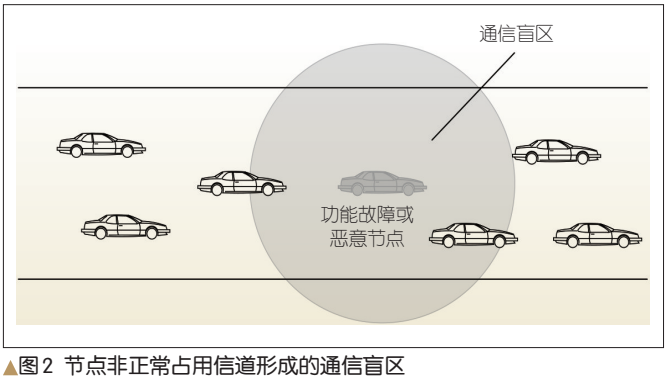
在本节中，我们提出相应的解决方案，以应对上述C-V2X的物理层安全问题。这些方案主要包括：单播通信中物理层安全通信方案和在终端自主资源分配模式下可能出现的持续非正常信道占用的解决方案。

2.1 单播通信中的物理层安全通信方案

在单播通信中，为了确定物理层数据只有源节点和目的节点能解码检测，可以对业务信道PSSCH的数据采用只有源节点和目的节点获知的专用标识进行加扰，其他周围节点



▲图1 恶意节点对单播通信的监测及干扰

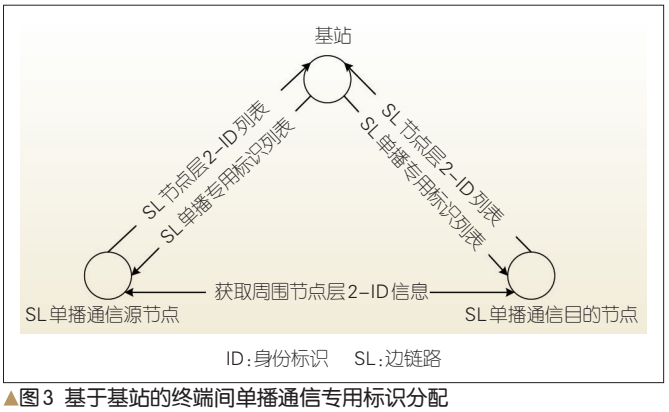


▲图2 节点非正常占用信道形成的通信盲区

由于未获知该专用标识则无法解扰该单播业务信道。一个实现方法就是借助基站为C-V2X通信指示用于单播通信的专用标识。具体流程可以设计为：终端节点获取周围节点的层2-ID信息，然后将获取的层2-ID信息连同自身的层2-ID信息形成一个节点层2-ID列表并上报给基站，基站依据上报的层2-ID为每两个节点之间的单播通信分配一个专用标识，最后基站将分配的单播专用标识发送给节点。如图3所示，假设图中源节点和目的节点的层2-ID分别为层2-ID1和层2-ID2，基站分别为层2-ID1和层2-ID2的节点之间的单播通信分配一个单播专用标识（专用标识1），并告知源节点和目的节点。源节点利用专用标识1加扰向目的节点发送的单播通信业务信道PSSCH，控制信道PSCCH中仍采用原广播模式下的加扰方式。源节点在PSCCH承载的SCI中直接指示单播通信源节点和目的节点相关的ID信息（一般为节点层2-ID的部分比特信息）。目的节点在检测到SCI中的ID信息之后，如果和自身的ID匹配，则进一步用和源节点层2-ID1、目的节点层2-ID2对应的单播专用标识1解扰业务信道。为节省信令开销，节点向基站上报的节点层2-ID信息可以是24 bit的层2-ID的部分比特信息。由于除源节点和目的节点之外的其他节点未获知源节点和目的节点之间单播专用标识1，因此这些节点无法解扰业务信道PSSCH，从而无法检测相应的单播通信物理层数据。

同样地，假设目的节点周围有一个恶意节点在SCI中指示目的节点的ID信息，并计划向其发送干扰信息。此时，即使目的节点判断该ID和自身相匹配，由于之前该节点未分配可信的单播专用标识，该目的节点仍可以不做接收检测处理。

此外，在设备准入的时候，测试终端可以作为非目的节点对接收数据的处理单元。如果设备可以正常对相应的物理层数据做丢弃处理，那么该设备就能满足准入条件。



▲图3 基于基站的终端间单播通信专用标识分配

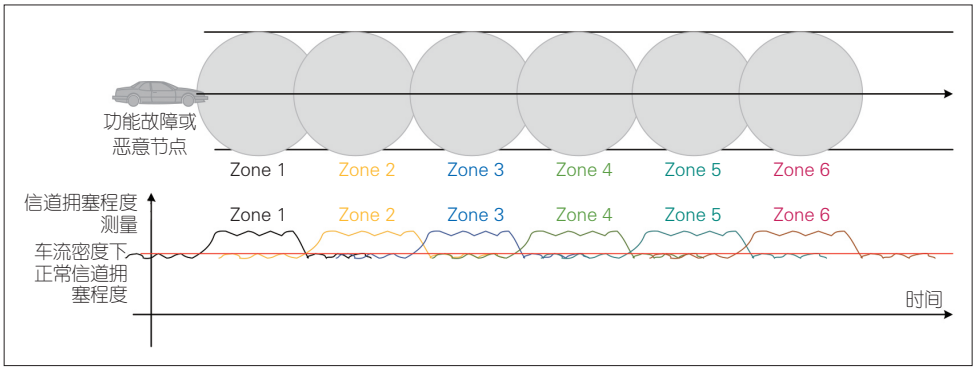
信道的节点是一个移动节点，则该节点移动经过的区域周围节点将无法接入信道或者传输会大量失败。如果这些周期节点将移动区域的信道接入状态或者传输状态上报给网络，那么网络可以通过历史信道拥塞程度的学习分析识别出通信故障区域。如图4所示，Zone 1至Zone 6在正常状态下可以通过历史数据识别一定车流密度下的正常信道拥塞程度。假设一个功能故障或者恶意节点从Zone1沿着道路移动到Zone 6，则Zone 1至Zone 6的信道拥塞程度会在该节点停留的时间内出现一个超预期的非正常状态，从而可判断Zone 1至Zone 6区域内存在一个故障或者恶意节点。结合车流的监控，我们可以进一步排查该节点。

在加强可信设备准入的监管方面，需要制定相应的设备拥塞控制和资源抢占功能测试标准，以测试设备是否依据标准中规定的拥塞控制机制配置相应的发送参数来占用信道，是否正常根据优先级和信道测量来抢占信道，以及是否按照标准规定配置资源抢占相关的参数，例如测试物理层SCI中优先级配置与高层业务之间的QoS映射是否正常等。在蜂窝覆盖区域，当基站根据用户设备（UE）上报的网络拥塞程度更改基于基站调度模式和基于终端自主资源分配模式的资源池配置和拥塞控制配置的参数时，系统将测试非基站连接下的终端是否可以通过边链路及时更改相关参数配置。例

2.2 持续非正常信道占用的解决方案

在基于终端自主的资源分配模式下，功能故障或者恶意持续超标占用信道会引起信道拥塞和通信盲区的问题。而这一问题很难被实时解决。对此，一方面可以通过上报并分析识别功能故障或者恶意节点的方式，另一方面也可以通过加强可行设备信道准入监管的方式来解决这类问题。

如果持续超标准非正常抢占



▲图4 异常区域信道拥塞程度监测

如，当基于终端自主资源分配模式的信道拥塞导致更多传输依靠基站调度时，基站可以增加基于基站调度的资源池数量，调整终端自主资源分配模式下的拥塞控制相关配置参数（相应的参数配置需及时应用于终端间通信）。

3 结束语

本文介绍了C-V2X目前主要面临的物理层安全问题，主要包括终端对单播通信物理层数据的检测获取，以及基于终端自主资源分配模式的信道拥塞和非正常资源抢占问题。对于5G NR-V2X中引入的单播通信问题，为避免其他终端的监测，可以借助基站为单播通信分配专用的标识，并在设备准入测试中测试设备对其作为非目的节点数据的处理功能是否正常来解决。对于基于终端自主资源分配模式下的非正常信道占用和资源抢占问题，则可以通过信道拥塞程度的监测来识别非正常区域以及该区域中的功能故障或者恶意节点，并借助设备拥塞控制和资源抢占功能的测试来解决。

致谢

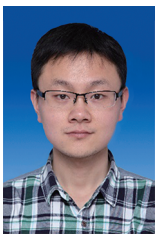
感谢北京邮电大学泛网无线通信教育部重点实验室的冯志勇教授与尉志青副教授对本研究的指导与帮助。

参考文献

[1] 曹雅丽. 车联网身份认证和安全信任体系亟待完善 [N]. 中国工业报, 2021-09-17(3)
[2] 董志国, 吴冬升. 智能网联汽车网络安全标准进展概述 [J]. 智能网联汽车, 2021(4): 52-56
[3] 工业和信息化部. 基于LTE的车联网通信安全技术要求: YD/T 3594-2019 [S]. 2019
[4] 3GPP. Security aspects of 3GPP support for advanced vehicle-to-everything (V2X) services: 3GPP TS 33.536 [S]. 2021
[5] 3GPP. Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation: 3GPP TS 36.211 [S]. 2021
[6] 3GPP. NR; physical channels and modulation: 3GPP TS 38.211 [S]. 2021
[7] 3GPP. NR; multiplexing and channel coding: 3GPP TS 38.212 [S]. 2021
[8] 3GPP. Evolved universal terrestrial radio access (E-UTRA); medium access control (MAC) protocol specification: 3GPP TS 36.321 [S]. 2021
[9] 3GPP. NR; medium access control (MAC) protocol specification: 3GPP TS 38.321 [S]. 2021
[10] 3GPP. NR; physical layer procedures for data: 3GPP TS 38.214 [S]. 2021

作 者 简 介

沈霞，中国信息通信研究院高级工程师；主要从事5G和无线局域网（WLAN）标准技术研究工作，参与完成IMT-2020（5G）推进组5G技术研发试验规范制定、5G新型多址和下一代WLAN等国家重大专项工作，对5G V2X、随机接入、NTN等3GPP标准课题开展有深入研究；申请专利40余项。



周伟，中国信息通信研究院工程师；主要从事5G的标准技术研究和仿真平台开发工作。

王志勤，中国信息通信研究院副院长、中国通信标准化协会无线通信技术工作委员会主席、中国通信学会无线及移动通信委员会主任委员，教授级高级工程师，“新一代宽带无线移动通信网”国家科技重大专项副总工程师；主要研究方向为无线移动通信技术和标准。