(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111148070 B
(45)授权公告日 2021.06.15

(21)申请号 201911403731.X
(22)申请日 2019.12.31
(65)同一申请的已公布的文献号
申请公布号 CN 111148070 A
(43)申请公布日 2020.05.12
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 虞靖靓 戴仕全 张浩
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 杨俊辉 臧建明
(51)Int.Cl.
H04W 4/40(2018.01)
H04W 12/00(2021.01)
H04W 12/37(2021.01)

(56)对比文件
CN 106845279 A,2017.06.13
CN 109714344 A,2019.05.03
CN 107392055 A,2017.11.24
CN 110366130 A,2019.10.22
CN 105791284 A,2016.07.20
CN 108881486 A,2018.11.23
CN 109348509 A,2019.02.15
CN 110532766 A,2019.12.03
US 2019311141 A1,2019.10.10
EP 3293656 A1,2018.03.14
李宁宁.基于机器学习的车联网入侵检测技术的研究与实现.《中国优秀硕士学位论文全文数据库工程科技Ⅱ辑》.2019,

审查员 张亚莉

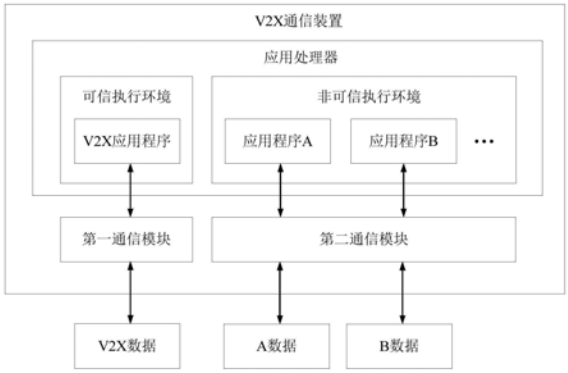
权利要求书2页 说明书14页 附图11页

(54)发明名称

V2X通信方法、装置及车辆

(57)摘要

本申请提供一种V2X通信方法、装置及车辆，其中在V2X通信装置的AP处理器中同时运行TEE和REE，AP处理器中的用于进行V2X通信的V2X应用程序全都运行在TEE中，从而将V2X应用程序与其他应用程序隔离，使得V2X应用程序能够在TEE中独立地处理V2X数据，通过TEE保证了V2X应用程序在处理V2X数据时不会被其他应用程序所影响或攻击，从而保证了运行在TEE中的V2X应用程序收发V2X数据时的安全，由于本申请提供的V2X通信装置能够在一个AP处理器上运行的TEE即可提高V2X应用程序进行V2X通信时的安全性能，并且不需要再设置单独的处理器，从而简化了V2X通信装置的结构，还能够降低硬件成本。



CN 111148070 B

1.一种车辆到一切V2X通信装置,设置在车辆上,其特征在于,所述装置包括:

AP处理器,所述AP处理器上运行有可信执行环境和非可信执行环境,所述可信执行环境用于运行V2X应用程序,所述非可信执行环境用于运行除所述V2X应用程序外的其他应用程序;

第一通信模块,用于被所述可信执行环境中运行的所述V2X应用程序调用时,发送或接收所述V2X应用程序的数据;

第二通信模块,用于被所述非可信执行环境中运行的所述其他应用程序调用时,发送或接收所述其他应用程序的数据。

2.根据权利要求1所述的装置,其特征在于,

所述可信执行环境还用于,对所述第一通信模块接收到的所述V2X应用程序的第一V2X数据进行安全校验;

若安全校验通过,所述V2X应用程序对所述第一V2X数据进行处理。

3.根据权利要求1所述的装置,其特征在于,还包括:

硬件安全模块HSM,与所述AP处理器连接,用于对所述第一通信模块接收到的所述V2X应用程序的第一V2X数据进行安全校验;

若安全校验通过,所述V2X应用程序对所述第一V2X数据进行处理。

4.根据权利要求1所述的装置,其特征在于,还包括:

硬件安全模块HSM,与所述第一通信模块连接,用于对所述第一通信模块接收到的所述V2X应用程序的第一V2X数据进行安全校验;

若安全校验通过,所述第一通信模块将所述第一V2X数据发送至所述可信执行环境。

5.根据权利要求2所述的装置,其特征在于,

所述可信执行环境还用于,对所述V2X应用程序生成的第二V2X数据进行加密;

所述第一通信模块具体用于发送经过加密后的所述第二V2X数据。

6.根据权利要求3所述的装置,其特征在于,

所述HSM还用于对所述V2X应用程序生成的第二V2X数据进行加密;

所述第一通信模块具体用于发送经过加密后的所述第二V2X数据。

7.根据权利要求4所述的装置,其特征在于,

所述HSM还用于对所述V2X应用程序生成的第二V2X数据进行加密;

所述第一通信模块具体用于发送经过加密后的所述第二V2X数据。

8.根据权利要求1-7任一项所述的装置,其特征在于,还包括:第一外部接口和第二外部接口;

所述第一外部接口用于被所述可信执行环境调用时,向连接的外部设备传输所述V2X应用程序的数据;

所述第二外部接口用于被所述非可信执行环境调用时,向连接的外部设备传输所述其他应用程序的数据。

9.根据权利要求8所述的装置,其特征在于,还包括:

数据获取单元,能够被所述可信执行环境调用,用于获取表示所述车辆状态的状态数据。

10.根据权利要求9所述的装置,其特征在于,

所述V2X应用程序具体用于,根据所述状态数据和第一V2X数据,生成处理结果,并通过所述第一外部接口发送所述处理结果。

11.根据权利要求8所述的装置,其特征在于,

所述V2X应用程序具体用于,通过所述第一外部接口发送第一V2X数据。

12.根据权利要求9所述的装置,其特征在于,

所述V2X应用程序具体用于,通过所述状态数据生成第二V2X数据。

13.一种车辆到一切V2X通信方法,其特征在于,应用于V2X通信装置中的AP处理器,其中,所述V2X通信装置包括:所述AP处理器,以及分别与所述AP处理器连接的第一通信模块和第二通信模块,所述AP处理器上运行有可信执行环境和非可信执行环境,所述可信执行环境用于运行V2X应用程序,所述非可信执行环境用于运行除所述V2X应用程序外的其他应用程序;所述方法包括:

所述AP处理器通过所述可信执行环境中运行的V2X应用程序,调用所述第一通信模块发送或接收所述V2X应用程序的数据;和/或,

所述AP处理器通过所述非可信执行环境中运行的所述其他应用程序,调用所述第二通信模块发送或接收所述其他应用程序的数据。

14.根据权利要求13所述的方法,其特征在于,所述方法还包括:

所述AP处理器通过所述可信执行环境对所述第一通信模块接收到的所述V2X应用程序的第一V2X数据进行安全校验。

15.根据权利要求13所述的方法,其特征在于,所述方法还包括:

所述AP处理器通过所述可信执行环境调用硬件安全模块HSM,对所述第一通信模块接收到的所述V2X应用程序的第一V2X数据进行安全校验。

16.根据权利要求14所述的方法,其特征在于,所述方法还包括:

所述AP处理器通过所述可信执行环境,对所述V2X应用程序生成的第二V2X数据进行加密。

17.根据权利要求15所述的方法,其特征在于,所述方法还包括:

所述AP处理器通过所述可信执行环境,调用硬件安全模块HSM,对所述V2X应用程序生成的第二V2X数据进行加密。

18.根据权利要求13-17任一项所述的方法,其特征在于,所述V2X通信装置还包括:分别与所述AP处理器连接的第一外部接口和第二外部接口;所述方法还包括:

所述AP处理器通过所述可信执行环境中运行的所述V2X应用程序,调用所述第一外部接口,向所述第一外部接口连接的外部设备传输所述V2X应用程序的数据;和/或,

所述AP处理器通过所述非可信执行环境中运行的所述其他应用程序,调用所述第二外部接口,向所述第二外部接口连接的外部设备传输所述其他应用程序的数据。

19.根据权利要求18所述的方法,其特征在于,所述V2X通信装置还包括:与所述AP处理器连接的数据获取单元,用于获取标识所述车辆状态的状态数据;所述方法还包括:

所述AP处理器通过所述可信执行环境中运行的所述V2X应用程序,根据所述状态数据和第一V2X数据,生成处理结果,并调用所述第一外部接口发送所述处理结果。

20.一种车辆,包括如权利要求1-12任一项所述的车辆到一切V2X通信装置。

V2X通信方法、装置及车辆

技术领域

[0001] 本申请涉及车辆网技术领域，尤其涉及一种车辆到一切(vehicle to everything，V2X)通信方法、装置及车辆。

背景技术

[0002] 随着网络技术及智能车辆技术的发展，车联网越来越受到广泛关注。目前，在车联网通信系统中，车辆到一切(vehicle to everything，V2X)通信装置(或称为车联网终端)设置在车辆内部，通过车用无线通信技术实现V(车)与X(车、人、交通路侧基础设施和网络)智能信息的交互。

[0003] 由于V2X通信数据与车辆的安全密切相关，也就需要保证V2X通信装置进行V2X通信时数据的安全。在一种技术中，发送数据的V2X通信装置可以使用密钥对V2X数据加密后进行发送，相应地，接收数据的V2X通信装置可以使用密钥对V2X数据解密后进行处理，但是在这种技术中由于V2X通信装置本身的安全性能较低，在V2X通信装置内部其他应用程序可能提供威胁V2X通信装置进行V2X通信的应用程序的入口，从而降低了V2X通信的安全。而在另一种技术中，V2X通信装置内可以设置两个不同的处理器，一个处理器处理V2X通信相关的应用程序，另一个处理器处理其他应用程序，从物理上对V2X通信进行隔离，但是这种技术极大地提高了V2X通信装置的硬件成本。

[0004] 因此，如何使V2X通信装置降低硬件成本的同时还能够提高安全性能，是本领域亟需解决的技术问题。

发明内容

[0005] 本申请提供一种V2X通信方法、装置及车辆，以解决现有技术中V2X通信装置不能在降低硬件成本的同时，还能够提高安全性能的技术问题。

[0006] 本申请第一方面提供一种V2X通信装置，包括：AP处理器，以及分别与AP处理器连接的第一通信模块和第二通信模块，AP处理器上运行有可信执行环境和非可信执行环境，可信执行环境用于运行V2X应用程序，非可信执行环境用于运行除V2X应用程序外的其他应用程序。具体地，AP处理器的可信执行环境中运行的V2X应用程序，可以通过调用第一通信模块发送或接收V2X应用程序；而AP处理器的非可信执行环境中运行的其他应用程序，可以通过调用第二通信模块发送或接收其他应用程序的数据。

[0007] 因此，本实施例提供的V2X通信装置，在AP处理器中同时运行TEE和REE，而AP处理器中的用于进行V2X通信的V2X应用程序全都运行在TEE中，因此将V2X应用程序与其他应用程序隔离，使得V2X应用程序能够在TEE中独立地处理V2X数据，通过TEE保证了V2X应用程序在处理V2X数据时不会被其他应用程序所影响或攻击；同时，运行在TEE中的V2X应用程序还可以调用同样独立设置的第一通信模块实现V2X数据的接收或发送，使得V2X应用程序使用的数据收发模块只能被TEE中的应用程序调用，从而与REE中其他应用程序能够调用的第二通信模块隔离，进一步保证了运行在TEE中的V2X应用程序收发V2X数据时的安全。综上，本

实施例提供的V2X通信装置，能够在一个AP处理器上运行的TEE即可提高V2X应用程序进行V2X通信时的安全性能，并且不需要再设置单独的处理器，从而简化了V2X通信装置的结构，还能够降低硬件成本。

[0008] 在本申请第一方面一实施例中，所述可信执行环境中V2X应用程序除了接收或发送V2X应用程序，V2X应用程序还可以在可信执行环境中，对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验；而当安全校验通过，V2X应用程序对第一V2X数据进行处理；当安全校验不通过，V2X应用程序不会继续对第一V2X数据进行处理。可选地，同时，V2X应用程序还可以在可信执行环境中，对待发送的第二V2X数据进行加密，并将加密后的第二V2X数据通过第一通信模块发送。

[0009] 因此，本实施例提供的V2X通信装置，当V2X应用程序在TEE中进行数据的接收或发送时，能够进一步在TEE中对数据进行加密、签名，或者在TEE中对数据进行解密、安全校验的操作，能够进一步保证了V2X应用程序所处理的V2X数据的安全。

[0010] 在本申请第一方面一实施例中，V2X通信装置中还包括：与AP处理器连接的HSM，用于对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验；即，V2X通信装置可以调用AP处理器连接的HSM对接收到的第一V2X数据进行安全校验；而当安全校验通过，V2X应用程序对第一V2X数据进行处理；当安全校验不通过，V2X应用程序不会继续对第一V2X数据进行处理。可选地，同时，V2X应用程序还可以在可信执行环境中，调用HSM对待发送的第二V2X数据进行加密，并将加密后的第二V2X数据通过第一通信模块发送。

[0011] 综上，本实施例提供的V2X通信装置，可以根据实际使用情况，在AP处理器之外设置独立的HSM，进行V2X数据的加密解密、签名以及验证等安全操作，从而减少AP处理器的运算量，并且HSM被配置为仅仅能够被TEE中的应用程序调用，还能够进一步保证了V2X应用程序在对V2X数据进行安全操作时的安全性能。

[0012] 在本申请第一方面一实施例中，V2X通信装置中所设置的HSM与第一通信模块中的V2X基带处理单元连接，并在V2X基带处理单元处理V2X数据时调用；即，V2X基带处理单元接收到第一V2X数据后，调用HSM对接收到的第一V2X数据进行安全校验；而当安全校验通过，V2X基带处理单元将第一V2X数据发送至V2X应用程序进行处理；当安全校验不通过，V2X应用程序不会将第一V2X数据发送至V2X应用程序。可选地，同时，V2X基带处理单元还可以对V2X应用程序待发送的第二V2X数据进行加密，并将加密后的第二V2X数据通过第一通信模块发送。

[0013] 综上，本实施例提供的V2X通信装置，同样可以根据实际使用情况，在AP处理器之外的V2X通信基带处理单元设置独立的HSM，使得V2X通信基带处理单元在V2X数据发送或接收过程中即可进行V2X数据的加密解密、签名以及验证等安全操作，从而减少AP处理器的运算量，并且HSM仅与第一通信模块中的V2X通信基带处理单元连接，而第一通信模块被配置为仅仅能够被TEE中的应用程序调用，还能够进一步保证了V2X应用程序在对V2X数据进行安全操作时的安全性能。

[0014] 在本申请第一方面一实施例中，V2X通信装置还包括：分别与AP处理器连接的第一外部接口和第二外部接口；其中，当第一外部接口被TEE中的V2X应用程序调用时，V2X应用程序可以通过该第一外部接口与第一外部设备之间传输数据。当第二外部接口被REE中的其他应用程序调用时，其他应用程序可以通过该第二外部接口与第二外部设备之间传输数

据。

[0015] 综上,本实施例提供的V2X通信装置中,TEE中运行的V2X应用程序所能够调用的外部接口与REE中运行的应用程序所能够调用的外部接口不同,从而将TEE和REE中运行的应用程序向外部设备发送数据时使用的外部接口进行物理隔离,使得V2X应用程序能够调用的物理接口本身是安全的,从而进一步保证了V2X应用程序在向外部发送V2X数据时的安全。

[0016] 在本申请第一方面一实施例中,V2X通信装置还包括:数据获取单元,能够被可信执行环境调用,用于获取表示车辆状态的状态数据。

[0017] 综上,本实施例提供的V2X通信装置,使得TEE环境中运行的V2X应用程序能够单独地调用确保安全的数据获取单元获取状态数据,该数据获取单元不会被REE中的应用程序调用,从而通过TEE保障V2X应用程序获取的状态数据安全,进一步保证了V2X应用程序处理V2X数据时的安全。

[0018] 在本申请第一方面一实施例中,V2X应用程序具体用于,根据状态数据和第一V2X数据,生成处理结果,并通过第一外部接口发送处理结果。

[0019] 综上,本实施例针对V2X通信装置接收到的第一V2X数据需要V2X应用程序处理,则V2X应用程序可以在通过TEE保障V2X应用程序获取的状态数据安全的情况下获取车辆的状态数据,还可以在通过TEE保障的第一V2X数据安全的情况下,生成处理结果,从而使得V2X应用程序能够进一步调用能够保障安全的第一外部接口发送处理结果,从而在V2X应用程序处理V2X数据的全过程通过TEE进行保护,进一步保证了V2X应用程序处理V2X数据时的安全。

[0020] 在本申请第一方面一实施例中,V2X应用程序具体用于,V2X应用程序具体用于,通过第一外部接口发送第一V2X数据。

[0021] 综上,本实施例针对V2X通信装置接收到的第一V2X数据是不需要V2X应用程序处理,而是直接进行转发,则V2X应用程序可以直接调用能够保障安全的第一外部接口将接收到的第一V2X数据转发,从而保证了V2X应用程序在转发V2X数据时的安全。

[0022] 在本申请第一方面一实施例中,V2X应用程序具体用于,V2X应用程序具体用于,通过状态数据生成第二V2X数据。

[0023] 综上,本实施例针对V2X通信装置自己根据车辆的状态数据生成待发送的第二V2X数据的过程,其中,由于V2X应用程序可以在通过TEE保障V2X应用程序获取的状态数据安全的情况下获取车辆的状态数据,还能够在TEE中生成第二V2X数据,随后进行发送。因此,在V2X应用程序生成、发送V2X数据的全过程通过TEE进行保护,进一步保证了V2X应用程序处理V2X数据时的安全。

[0024] 本申请第二方面提供一种V2X通信方法,可应用于本申请第一方面提供的V2X通信装置中的AP处理器,其中,方法包括:AP处理器通过可信执行环境中运行的V2X应用程序,调用第一通信模块发送或接收V2X应用程序的数据;和/或,AP处理器通过非可信执行环境中运行的其他应用程序,调用第二通信模块发送或接收其他应用程序的数据。

[0025] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验。

[0026] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境调

用硬件安全模块HSM,对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验。

[0027] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境,对V2X应用程序生成的第二V2X数据进行加密。

[0028] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境,调用硬件安全模块HSM,对V2X应用程序生成的第二V2X数据进行加密。

[0029] 在本申请第二方面一实施例中,V2X通信装置还包括:分别与AP处理器连接的第一外部接口和第二外部接口;所述方法还包括:AP处理器通过可信执行环境中运行的V2X应用程序,调用第一外部接口,向第一外部接口连接的外部设备传输V2X应用程序的数据;和/或,AP处理器通过非可信执行环境中运行的其他应用程序,调用第二外部接口,向第二外部接口连接的外部设备传输其他应用程序的数据。

[0030] 在本申请第二方面一实施例中,V2X通信装置还包括:与AP处理器连接的数据获取单元,用于获取标识车辆状态的状态数据;所述方法还包括:AP处理器通过可信执行环境中运行的V2X应用程序,根据状态数据和第一V2X数据,生成处理结果,并调用第一外部接口发送处理结果。

[0031] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境中运行的V2X应用程序,第一外部接口发送第一V2X数据。

[0032] 在本申请第二方面一实施例中,所述方法还包括:AP处理器通过可信执行环境中运行的V2X应用程序,通过状态数据生成第二V2X数据。

[0033] 有关第二方面提供的V2X通信方法的具体实现方式及有益效果,可参照本申请第一方面对于V2X通信装置的描述,不再赘述。

[0034] 本申请第三方面提供一种V2X通信装置,该V2X通信装置用于实现上述方法中的功能。所述功能可以通过硬件实现,也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

[0035] 本申请第四方面提供一种包含指令的计算机程序产品,当其运行时,使得V2X通信装置执行上述第二方面或第二方面的各种可能的实现方式中的方法。

[0036] 本申请第五方面提供一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,当其运行时,使得V2X通信装置执行上述第一方面或第一方面的各种可能的实现方式中的方法。

[0037] 本申请第六方面提供一种芯片系统,该芯片系统包括处理器,还可以包括存储器,用于实现上述方法中V2X通信装置的功能。该芯片系统可以由芯片构成,也可以包含芯片和其他分立器件。

[0038] 本申请第七方面提供一种车辆,包括如本申请第一方面任一实施例中的V2X通信装置。

[0039] 综上,本申请提供一种V2X通信方法、装置及车辆,其中在AP处理器中同时运行TEE和REE,而AP处理器中的用于进行V2X通信的V2X应用程序全都运行在TEE中,因此将V2X应用程序与其他应用程序隔离,使得V2X应用程序能够在TEE中独立地处理V2X数据,通过TEE保证了V2X应用程序在处理V2X数据时不会被其他应用程序所影响或攻击;同时,运行在TEE中的V2X应用程序还可以调用同样独立设置的第一通信模块实现V2X数据的接收或发送,使得V2X应用程序使用的数据收发模块只能被TEE中的应用程序调用,从而与REE中其他应用程

序能够调用的第二通信模块隔离，进一步保证了运行在TEE中的V2X应用程序收发V2X数据时的安全。综上，本实施例提供的V2X通信装置，能够在一个AP处理器上运行的TEE即可提高V2X应用程序进行V2X通信时的安全性能，并且不需要再设置单独的处理器，从而简化了V2X通信装置的结构，还能够降低硬件成本。

附图说明

[0040] 图1为本申请所应用场景的示意图；

[0041] 图2为一种V2X通信装置的结构示意图；

[0042] 图3为另一种V2X通信装置的结构示意图；

[0043] 图4为本申请提供的V2X通信装置一实施例的结构示意图；

[0044] 图5为本申请提供的应用处理器的软件架构示意图；

[0045] 图6为本申请提供的V2X通信装置一实施例的结构示意图；

[0046] 图7为本申请提供的V2X通信装置一实施例的结构示意图；

[0047] 图8为本申请提供的TEE中的软件结构示意图；

[0048] 图9示出了一种V2X数据的接收处理流程；

[0049] 图10示出了一种V2X数据的发送处理流程；

[0050] 图11为本申请提供的V2X通信装置一实施例的结构示意图；

[0051] 图12为本申请提供的TEE中的软件结构示意图；

[0052] 图13示出了一种V2X数据的接收处理流程；

[0053] 图14示出了一种V2X数据的发送处理流程。

具体实施方式

[0054] 下面在介绍本申请实施例之前，先结合附图，对本申请应用的场景以及该应用场景中存在的技术问题进行说明。

[0055] 图1为本申请所应用场景的示意图，如图1所示，本申请可应用在车辆网通信的应用场景中，其中，如图1所示的车辆为了进行通信，可以在车辆上设置V2X通信装置(或称为：车辆网终端)，通过所设置的V2X通信装置，图中的车辆可以与其他车辆进行车与车(vehicle to vehicle，V2V)通信，与其他行人进行车与行人(vehicle to pedestrian，V2P)通信，与其他路侧基础设备进行车与基础设施(vehicle to infrastructure，V2I)通信，或者通信网络进行车与网络(vehicle to network，V2N)通信。V2X通信能够实现车辆与行人、其他车辆、路侧设备、网络之间的全方位连接和高效信息交互，实现信息服务、交通安全、交通效率等功能。

[0056] 随着网络技术以及智能车辆技术的发展，车辆通过V2X通信装置能够实现的功能也越来越丰富，例如，V2X通信装置通过V2I和V2N通信可以获取各种信息服务，包括交通信号灯信息，附近区域车辆信息，车辆导航信息，紧急救援信息，娱乐服务信息等；V2X通信装置通过V2V和V2P通信可以实时获取周围车辆的车速、位置、行车情况及行人活动等信息，并通过智能算法实现碰撞预警功能，避免车辆发生交通事故；V2X通信装置通过V2I通信可以实现车速引导等功能以提高交通效率。

[0057] 由于V2X通信装置通过V2X通信所提供的服务与安全性能息息相关，一旦车辆使用

的V2X通信装置在通信过程中传输的数据被非法篡改或被仿冒，或者V2X通信装置上运行的V2X应用和算法过程被攻击，会严重影响车辆的正常行驶，甚至威胁道路上其他车辆和行人的安全，因此V2X通信装置需要在进行V2X通信以及提供相关服务时，保证其数据安全。

[0058] 在一些技术中，V2X通信装置在进行V2X通信时，可以对所传输的数据进行加密以保证数据安全。例如，图2为一种V2X通信装置的结构示意图，如图2所示，能够进行V2X通信的V2X应用程序可以运行在V2X通信装置中的应用处理器上，当所述V2X通信装置作为发送方发送V2X数据时，V2X应用程序通过密钥对V2X数据进行签名和加密后再通过通信模块进行发送；当所述V2X通信装置作为接收方接收V2X数据时，V2X应用程序通过通信模块接收到V2X数据后，还需要通过身份认证服务器获取对称密钥对V2X数据进行解密。从而在整个V2X数据的发送和接收的传输过程中，通过签名和加密的安全机制保护V2X数据不被篡改。

[0059] 然而，在如图2所示的技术中，由于V2X通信装置中的应用处理器除了运行V2X应用程序，还会同时运行其他应用程序，例如图中示例的应用程序A和应用程序B，应用程序A和B也会分别调用通信模块发送或接收A数据以及B数据。从而造成了应用处理器上运行的V2X应用程序在计算处理过程中，容易受到其他应用程序带来的攻击威胁，导致V2X应用程序异常而威胁车辆的安全。

[0060] 在另一些技术中，V2X通信装置中可以设置不同的应用处理器，使V2X应用程序与其他应用程序运行在不同的应用处理器内，实现V2X应用程序的隔离。例如，图3为另一种V2X通信装置的结构示意图，如图3所示，V2X通信装置中设置有应用处理器1和应用处理器2至少两个应用处理器，能够进行V2X通信的V2X应用程序在应用处理器1中运行，除V2X应用程序之外的其他应用程序在应用程序处理器2中运行。则当所述V2X通信装置发送或接收V2X数据时，V2X应用程序通过调用通信模块1发送或接收V2X数据，所述通信模块1可以集成在应用处理器1中，或者独立设置。相应地，应用处理器2中应用程序A和B可以调用通信模块发送或接收A数据和B数据。

[0061] 然而，在如图3所示的技术中，为了确保V2X应用程序的独立运行，V2X通信装置中需要设置至少两个应用处理器实现应用程序之间的硬件隔离，而由于目前处理器高昂的成本，V2X通信装置中设置的多个处理器极大地提高了整个V2X通信装置的成本。

[0062] 综上，V2X通信装置在如图2所示的技术中安全性能较差，而在图3所示的技术中硬件成本较高，上述两种技术都存在各自的不足，而如何使V2X通信装置降低件成本的同时，还能够提高安全性能，是本领域亟需解决的技术问题。

[0063] 因此，为了解决上述技术问题，本申请提供一种V2X通信方法及装置，以解决现有技术中V2X通信装置不能在降低硬件成本的同时，还能够提高安全性能的技术问题。下面结合附图，以具体地实施例对本申请的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0064] 图4为本申请提供的V2X通信装置一实施例的结构示意图，如图4所示，本申请提供的V2X通信装置可以设置在如图1所示的车辆上，用于如图1所示的车辆进行V2X通信。所述V2X通信装置包括：应用(application，AP)处理器，所述AP处理器上运行有可信执行环境(trusted execution environment，TEE)和非可信执行环境(rich execution environment，REE)。

[0065] 其中，所述TEE基于ARM Trustzone的安全技术，将操作系统隔离成两个世界，即安

全世界和非安全世界，通过硬件实现安全隔离，包括对外设的隔离，TEE是安全世界的软件运行环境，与非安全世界的软件运行环境REE之间具有类似于硬件级别的安全隔离机制，REE中运行的应用程序无法直接访问TEE中运行的应用程序。在本实施例中，AP处理器中运行的TEE用于运行用于进行V2X通信的V2X应用程序，同时，AP处理器中可以包括一个或多个V2X应用程序，AP处理器中的所有V2X应用程序都运行在TEE中，在图4中以V2X应用程序作为示例。AP处理器中运行的REE用于运行AP处理器中除V2X应用程序之外的应用程序，也就是不进行V2X通信的应用程序，本实施例中将除V2X应用程序之外的应用程序记为其他应用程序，在图4中以其他应用程序包括：应用程序A、应用程序B……作为示例。

[0066] 所述V2X通信装置还包括：第一通信模块和第二通信模块，其中，第一通信模块连接AP处理器，并且第一通信模块被配置为仅能够被TEE中运行的V2X应用程序调用、不能被REE中运行的其他应用程序调用，并在被调用时发送或接收V2X应用程序的V2X数据；第二通信模块也连接AP处理器，并且第二通信模块被配置为仅能够被REE中运行的其他应用程序调用、而不能被TEE中运行的V2X应用程序调用，并在被调用时发送或接收其他应用程序的数据。

[0067] 可选地，所述第一通信模块可以包括：V2X通信基带处理单元和V2X通信射频单元，其中，V2X通信基带处理单元支持V2X通信技术的基带处理功能，V2X通信射频单元支持V2X通信技术的射频信号处理功能。所述第一通信模块用于发送或接收V2X数据时，所支持的技术标准可以是基于WAVE技术(又称IEEE 802.11p)的DSRC标准，也可以是基于蜂窝技术的(cellular)C-V2X标准。所述第二通信模块可以包括：蜂窝通信基带处理单元和蜂窝通信射频单元，其中，蜂窝通信基带处理单元：支持蜂窝通信技术(2G/3G/4G/5G)的基带处理功能，蜂窝通信射频单元：支持蜂窝通信技术(2G/3G/4G/5G)的射频信号处理功能。

[0068] 进一步可选地，所述AP处理器和第二通信模块中的蜂窝基带处理器单元可以集成在同一个芯片上，所述芯片可以是系统级芯片(system on chip，SoC)，也可以是基带芯片；或者，蜂窝基带处理器单元和AP处理器还可以设置在独立的芯片上。或者，所述AP处理器、第二通信模块中的蜂窝基带处理单元，以及第一通信模块中的V2X基带处理单元可以集成在同一个芯片上，所述芯片可以是SoC，也可以是基带芯片；或者，蜂窝基带处理器单元、V2X基带处理单元和AP处理器还可以设置在独立的芯片上。所述V2X通信射频单元，可以设置在独立的芯片上，与V2X通信基带处理单元连接；或者，所述V2X通信射频单元还可以与蜂窝通信射频单元设置在同一个芯片上，所述芯片可以是SoC，也可以是蜂窝通信射频芯片。

[0069] 更为具体地，图5为本申请提供的应用处理器的软件架构示意图，其中，对于TEE中运行的V2X应用程序，运行在独立的安全OS中，处于应用层的V2X应用程序，或者V2X算法可以通过V2X协议栈以及安全服务，进一步调用第一通信模块发送或接收V2X数据。对于REE中运行的应用程序，运行在独立的OS中，处于应用层的应用程序同样可以通过中间件调用第二通信模块发送或接收数据。

[0070] 通过图4和图5可以看出，本实施例提供的V2X通信装置中可以设置一个AP处理器，而在该AP处理器中同时运行TEE和REE，而AP处理器中的用于进行V2X通信的V2X应用程序全都运行在TEE中，因此将V2X应用程序与其他应用程序隔离，使得V2X应用程序能够在TEE中独立地处理V2X数据，通过TEE保证了V2X应用程序在处理V2X数据时不会被其他应用程序所影响或攻击；同时，运行在TEE中的V2X应用程序还可以调用同样独立设置的第一通信模块

实现V2X数据的接收或发送，使得V2X应用程序使用的数据收发模块只能被TEE中的应用程序调用，从而与REE中其他应用程序能够调用的第二通信模块隔离，进一步保证了运行在TEE中的V2X应用程序收发V2X数据时的安全。因此，本申请提供的V2X通信装置，能够在一个AP处理器上运行的TEE即可提高V2X应用程序进行V2X通信时的安全性能，并且不需要再设置单独的处理器，从而简化了V2X通信装置的结构，还能够降低硬件成本。

[0071] 进一步地，在上述实施例中，V2X通信装置的TEE中运行的V2X应用程序在处理器V2X应用程序时，还可以对V2X数据进行加密或者安全校验的处理。其中，当TEE中运行的V2X应用程序作为数据接收方时，记V2X应用程序通过调用第一通信模块接收到的数据为第一V2X数据，则V2X应用程序首先对第一V2X数据进行安全检验以及解密处理，随后，V2X应用程序进一步对通过安全校验以及解密后的第一V2X数据进行处理；当TEE中运行的V2X应用程序作为数据发送方时，记V2X应用程序可以确定需要发送的数据为第二V2X数据，则V2X应用程序首先对第二V2X数据进行加密以及签名处理，随后，V2X应用程序调用第一通信模块将加密签名后的第二V2X数据进行发送。

[0072] 综上，本实施例提供的V2X通信装置，当V2X应用程序在TEE中进行数据的接收或发送时，能够进一步在TEE中对数据进行加密、签名，或者在TEE中对数据进行解密、安全校验的操作，能够进一步保证了V2X应用程序所处理的V2X数据的安全。

[0073] 或者，在另一种可能的实现方式中，V2X通信装置中还可以设置硬件安全模块(hardware security module，HSM)，V2X应用程序可以通过调用HSM对接收到的V2X数据进行校验。其中，所述HSM支持安全算法处理、密钥以及数据的安全存储。例如，图6为本申请提供的V2X通信装置一实施例的结构示意图，如图6所示的V2X通信装置在图4所示实施例的基础上，还包括与AP处理器连接的HSM，所述HSM被配置为能够被TEE中的应用程序调用，而不能对REE中的应用程序调用。则对于如图6所示的V2X通信装置，作为数据接收方在接收到第一V2X数据后，调用HSM对第一V2X数据进行安全校验以及解密处理，HSM将处理后的第一V2X数据发送至V2X应用程序，对于TEE中的V2X应用程序即可不需要对第一V2X数据进行解密以及安全校验，可以直接处理第一V2X数据；同样地，当如图6所示的V2X通信装置作为数据发送方生成待发送的第二V2X数据后，调用HSM对第二V2X数据进行加密以及签名处理，HSM将处理后的第二V2X数据发送至V2X应用程序，对于TEE中的V2X应用程序即可不需要对第二V2X数据进行加密以及签名，可以直接调用第一通信模块发送所述第二V2X数据。

[0074] 综上，本实施例提供的V2X通信装置，可以根据实际使用情况，在AP处理器之外设置独立的HSM，进行V2X数据的加密解密、签名以及验证等安全操作，从而减少AP处理器的运算量，并且HSM被配置为仅仅能够被TEE中的应用程序调用，还能够进一步保证了V2X应用程序在对V2X数据进行安全操作时的安全性能。

[0075] 或者，在又一种可能的实现方式中，V2X通信装置中所设置的HSM与第一通信模块中的V2X基带处理单元连接，并在V2X基带处理单元处理V2X数据时调用。例如，当V2X通信装置作为数据接收方，在V2X基带处理单元接收到第一V2X数据后，调用HSM对第一V2X数据进行安全校验以及解密处理，HSM将处理后的第一V2X数据发送至V2X基带处理单元，再由V2X基带处理单元将第一V2X数据发送至TEE中的V2X应用程序处理；当V2X通信装置作为数据发送方，V2X应用程序生成待发送的第二V2X数据，调用V2X基带处理单元进行发送时，V2X基带处理单元首先调用HSM对第二V2X数据进行加密以及签名处理，HSM将处理后的第二V2X数据

发送至V2X基带处理单元，则V2X基带处理单元将处理后的第二V2X数据发送至V2X射频单元发送。

[0076] 综上，本实施例提供的V2X通信装置，同样可以根据实际使用情况，在AP处理器之外的V2X通信基带处理单元设置独立的HSM，使得V2X通信基带处理单元在V2X数据发送或接收过程中即可进行V2X数据的加密解密、签名以及验证等安全操作，从而减少AP处理器的运算量，并且HSM仅与第一通信模块中的V2X通信基带处理单元连接，而第一通信模块被配置为仅仅能够被TEE中的应用程序调用，还能够进一步保证了V2X应用程序在对V2X数据进行安全操作时的安全性能。

[0077] 进一步地，上述各实施例针对V2X通信装置中，针对在TEE中运行V2X应用程序接收、发送V2X数据以及处理V2X数据的过程，以保证V2X应用程序进行V2X通信时的安全。而当V2X应用程序需要进一步向V2X通信装置之外的设备发送数据，或者需要接收V2X通信装置之外的设备发送的数据时，由于V2X应用程序设置在TEE之中，因此也还需要对其他设备的物理接口或者通信接口进行相应的配置，以进一步保证V2X应用程序在处理V2X数据时的安全。

[0078] 例如，图7为本申请提供的V2X通信装置一实施例的结构示意图，如图7所示的V2X通信装置在如图6所示实施例的基础上，还将V2X通信装置所具有的多个外部物理接口进一步划分为第一外部接口和第二外部接口。其中，所述外部物理接口的具体实现形式包括但不限于：以太网(ethernet)接口、无线保真(wireless fidelity，Wi-Fi)接口以及通用串行总线(universal serial bus，USB)接口。

[0079] 其中，将第一外部接口连接的外部设备记为第一外部设备，第一外部接口被配置为能够被TEE中的应用程序调用，而不能够被REE中的应用程序调用；当第一外部接口被TEE中的V2X应用程序调用时，V2X应用程序可以通过该第一外部接口与第一外部设备之间传输数据。将第二外部接口连接的外部设备记为第二外部设备，第二外部接口被配置为能够被REE中的应用程序调用，而不能够被TEE中的应用程序调用；当第二外部接口被REE中的其他应用程序调用时，其他应用程序可以通过该第二外部接口与第二外部设备之间传输数据。即，本申请实施例中将V2X通信装置的外部接口分别划分给TEE和REE调用，从而将TEE和REE中运行的应用程序向外部设备发送数据时使用的外部接口进行物理隔离。

[0080] 如图7所示的V2X通信单元还可以包括：数据获取单元，数据获取单元被配置为仅能够被TEE中的应用程序调用，而不能够被REE中的应用程序调用；当数据获取单元被TEE中的V2X应用程序调用时，V2X应用程序可以通过数据获取单元获取用于表示车辆状态的状态数据。

[0081] 可选地，在图7所示的示例中，TEE中V2X应用程序可以调用的数据获取单元可以包括：控制器局域网络(controller area network，CAN)数据单元、全球导航卫星系统(global navigation satellite system，GNSS)数据单元以及传感器单元。其中，CAN数据单元包括支持CAN的微控制单元(microcontroller unit，MCU)和CAN收发器组成的CAN数据单元，用于获取V2X通信装置所在车辆的车速，转向，刹车等行驶数据；GNSS数据单元支持GNSS定位功能，GNSS数据单元可以是独立的芯片，或者还可以集成在应用处理器所在的芯片中；传感器数据单元，可以包括例如：陀螺仪和加速度传感器等，用于获取车辆的实时状态数据，所述传感器数据单元可以是独立的芯片，或者还可以集成在应用处理器所在的芯

片中，又或者与GNSS芯片连接。

[0082] 综上，本实施例提供的V2X通信装置中，TEE中运行的V2X应用程序所能够调用的外部接口与REE中运行的应用程序所能够调用的外部接口不同，从而将TEE和REE中运行的应用程序向外部设备发送数据时使用的外部接口进行物理隔离，使得V2X应用程序能够调用的物理接口本身是安全的，从而进一步保证了V2X应用程序在向外部发送V2X数据时的安全。

[0083] 更为具体地，图8为本申请提供的TEE中的软件结构示意图，其中示出了如图7所示的V2X通信装置中，TEE中运行的V2X应用程序调用相关模块进行数据传输的软件模块关系。其中，V2X应用处理模块用于运行V2X应用程序，V2X网络传输协议处理模块用于处理V2X数据，V2X网络传输协议处理模块可以通过V2X安全模块调用安全服务器模块(HSM)对V2X数据进行安全操作，V2X接入层协议处理模块用于发送或接收V2X数据，V2X算法处理模块用于通过车辆数据模块、车辆位置模块等数据获取单元获取车辆的状态数据。

[0084] 如图8所示的软件结构一种具体的应用为第一V2X数据的接收过程，例如，图9示出了一种V2X数据的接收处理流程，其中，当流程开始后，V2X接入层协议处理模块接收第一V2X数据，并将接收到的第一V2X数据通过物理接口或者核间通信接口发送至TEE中运行的V2X网络传输协议处理模块。V2X网络传输协议处理模块将第一V2X数据发送至V2X安全模块进行签名验证和解密，具体地，V2X安全模块可以调用安全服务器块对第一V2X数据进行签名验证和解密，其中，当对第一V2X数据签名验证未通过，则结束流程；当对第一V2X数据签名验证通过后，将通过签名验证以及解密后的第一V2X数据发送至V2X应用处理模块进行进一步处理。

[0085] V2X应用处理模块在接收到第一V2X数据之后，需要对该第一V2X数据是否需要本地处理进行判断。例如，对于一些需要V2X通信装置直接转发给其他车辆或者设备的通知信息数据，V2X应用处理模块判断本地不需要进行计算处理，则直接将接收到的第一V2X数据通过调用外部接口发送给外部设备。对于一些需要V2X通信装置进一步结合自身车辆状态进行处理的数据，V2X应用处理模块在判断本地需要将进行计算处理后，将接收到的第一V2X数据发送至V2X算法处理模块，由V2X算法处理模块结合从车辆数据模块、位置数据模块获取的本车车速、转向、刹车、位置等数据进行计算后，得到计算后的处理结果例如碰撞预警信息，并返回V2X应用处理模块。最终，V2X应用处理模块将得到的处理结果通过外部通信接口发送至外部设备，从而结束流程。

[0086] 如图8所示的软件结构另一种具体的应用为第二V2X数据的发送过程，例如，图10示出了一种V2X数据的发送处理流程，其中，当流程开始后，V2X应用处理模块可以按照一定的周期生成待发送的第二V2X数据，具体由V2X算法处理模块从车辆数据模块和位置数据模块获取车速、位置等数据后，生成一条待发送的第二V2X数据。随后，由V2X应用处理模块将第二V2X数据发送给V2X网络传输协议处理模块进行发送，而V2X网络传输协议处理模块通过V2X安全模块调用安全服务模块对第二V2X数据进行签名和加密处理后，V2X网络传输协议模块将处理后的第二V2X数据通过物理接口或者核间通信接口发送给V2X接入层协议处理模块。最终，由V2X接入层协议处理模块在空口发送所述第二V2X数据，从而结束流程。

[0087] 可选地，上述如图8-10所示的实施例中提供的V2X通信装置所设置的HSM与AP处理器的TEE连接并能够被TEE中运行的V2X应用程序调用，在本申请其他可能的实现方式中，

V2X通信装置所设置的HSM可以与第一通信模块中的V2X基带处理单元连接，并能够被V2X基带处理单元调用。例如，图11为本申请提供的V2X通信装置一实施例的结构示意图，如图11所示的V2X通信装置与如图7所示的V2X通信装置存在的区别在于，HSM与第一通信模块中的V2X基带处理单元连接。

[0088] 具体地，图12为本申请提供的TEE中的软件结构示意图，其中示出了如图11所示的V2X通信装置中，TEE中运行的V2X应用程序调用相关模块进行数据传输的软件模块关系。其中，V2X应用处理模块用于运行V2X应用程序，V2X网络传输协议处理模块用于处理V2X数据，V2X接入层协议处理模块用于发送或接收V2X数据，V2X接入层协议处理模块可以调用V2X安全模块(HSM)对V2X数据进行安全操作，V2X算法处理模块用于通过车辆数据模块、车辆位置模块等数据获取单元获取车辆的状态数据。

[0089] 如图12所示的软件结构一种具体的应用为第一V2X数据的接收过程，例如，图13示出了一种V2X数据的接收处理流程，其中，当流程开始后，V2X接入层协议处理模块接收第一V2X数据，并将接收到的第一V2X数据调用V2X安全模块进行解密和签名验证。其中，当对第一V2X数据签名验证未通过，则结束流程；当对第一V2X数据签名验证通过后，通过物理接口或者核间通信接口，将通过签名验证以及解密后的第一V2X数据发送至TEE中运行的V2X网络传输协议处理模块。V2X网络传输协议处理模块进一步将第一V2X数据发送至V2X应用处理模块进行进一步处理。同样地，V2X应用处理模块在接收到第一V2X数据之后，需要对该第一V2X数据是否需要本地处理进行判断。有有关V2X应用处理模块进对第一V2X数据进行的处理可参照如图9所示的实施例，不再赘述。

[0090] 如图12所示的软件结构另一种具体的应用为第二V2X数据的发送过程，例如，图14示出了一种V2X数据的发送处理流程，其中，当流程开始后，V2X应用处理模块可以按照一定的周期生成待发送的第二V2X数据，具体由V2X算法处理模块从车辆数据模块和位置数据模块获取车速、位置等数据后，生成一条待发送的第二V2X数据。随后，由V2X应用处理模块将第二V2X数据发送给V2X网络传输协议处理模块进行发送，V2X网络传输协议处理模块将第二V2X数据通过物理接口或者核间通信接口发送至V2X接入层协议处理模块。V2X接入层协议处理模块能够通过V2X安全模块调用安全服务模块对第二V2X数据进行签名和加密处理后，在空口发送所述第二V2X数据，从而结束流程。

[0091] 进一步地，本申请还提供一种V2X通信方法，可以由上述任意实施例中的AP处理器执行，示例性地，所述V2X通信方法可以包括：AP处理器通过可信执行环境中运行的V2X应用程序，调用第一通信模块发送或接收V2X应用程序的数据；和/或，AP处理器通过非可信执行环境中运行的其他应用程序，调用第二通信模块发送或接收其他应用程序的数据。

[0092] 或者，可选地，所述方法还包括：AP处理器通过可信执行环境对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验。

[0093] 可选地，所述方法还包括：AP处理器通过可信执行环境调用硬件安全模块HSM，对第一通信模块接收到的V2X应用程序的第一V2X数据进行安全校验。

[0094] 可选地，所述方法还包括：AP处理器通过可信执行环境，对V2X应用程序生成的第二V2X数据进行加密。

[0095] 可选地，所述方法还包括：AP处理器通过可信执行环境，调用硬件安全模块HSM，对V2X应用程序生成的第二V2X数据进行加密。

[0096] 可选地，所述方法还可以包括：AP处理器通过可信执行环境中运行的V2X应用程序，调用第一外部接口，向第一外部接口连接的外部设备传输V2X应用程序的数据；和/或，AP处理器通过非可信执行环境中运行的其他应用程序，调用第二外部接口，向第二外部接口连接的外部设备传输其他应用程序的数据。

[0097] 可选地，所述方法还包括：方法还包括：AP处理器通过可信执行环境中运行的V2X应用程序，根据状态数据和第一V2X数据，生成处理结果，并调用第一外部接口发送处理结果。

[0098] 可选地，所述方法还包括：AP处理器通过可信执行环境中运行的V2X应用程序，第一外部接口发送第一V2X数据。

[0099] 可选地，所述方法还包括：AP处理器通过可信执行环境中运行的V2X应用程序，通过状态数据生成第二V2X数据。

[0100] 需要说明的是，上述由AP处理器执行的方法，其执行主体还可以是AP处理器中对应的V2X应用程序，或者AP处理器中对应的其他应用程序。

[0101] 上述各实施例提供的V2X通信方法，其实现方式与原理可以参照本申请实施例中对于V2X通信装置所进行的说明，不再赘述。

[0102] 为了实现本申请实施例中提供的V2X通信方法，AP处理器的存储器中，可以存储计算机可执行程序代码，所述程序代码包括指令；当AP处理器执行指令时，指令使AP处理器执行上述实施例或可选实施例中AP处理器的处理动作，其实现原理和技术效果类似，在此不再赘述。或者，可选地，为了实现本申请实施例中的V2X通信方法，V2X通信装置中除AP处理器之外的各模块也可以存储计算机可执行程序代码，例如，如图11所示的V2X通信基带处理单元可以存储程序代码包括指令，当V2X通信基带处理单元执行指令时，可以使其执行由V2X通信基带处理单元执行的调用HSM等相关动作。

[0103] 本领域技术人员应该很容易意识到，结合本申请中所公开的实施例描述的各实施例的算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0104] 本申请实施例可以根据上述示例对V2X通信装置中模块的划分时，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。例如，第一通信模块和第二通信模块可以是两个不同的模块，或者集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0105] 本文中的术语“多个”是指两个或两个以上。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系；在公式中，字符“/”，表示前后关联对象是一种“相除”的关系。

[0106] 可以理解的是，在本申请的实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请的实施例的

实施过程构成任何限定。

[0107] 可以理解的是，在本申请的实施例中，存储器可以是非易失性存储器，比如硬盘(hard disk drive，HDD)或固态硬盘(solid-state drive，SSD)等，还可以是易失性存储器(volatile memory)，例如随机存取存储器(random-access memory，RAM)。存储器是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。本申请实施例中的存储器还可以是电路或者其它任意能够实现存储功能的装置，用于存储程序指令和/或数据。

[0108] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。

[0109] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个装置，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0110] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是一个物理单元或多个物理单元，即可以位于一个地方，或者也可以分布到多个不同地方。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0111] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0112] 本申请实施例提供的方法中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、网络设备、终端或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(digital subscriber line，DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机可以存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质(例如，软盘、硬盘、磁带)、光介质(例如，数字视频光盘(digital video disc，DVD))、或者半导体介质(例如，SSD)等。

[0113] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何在本申请揭露的技术范围内的变化或替换，都应涵盖在本申请的保护范围之内。因此，本申

请的保护范围应以所述权利要求的保护范围为准。

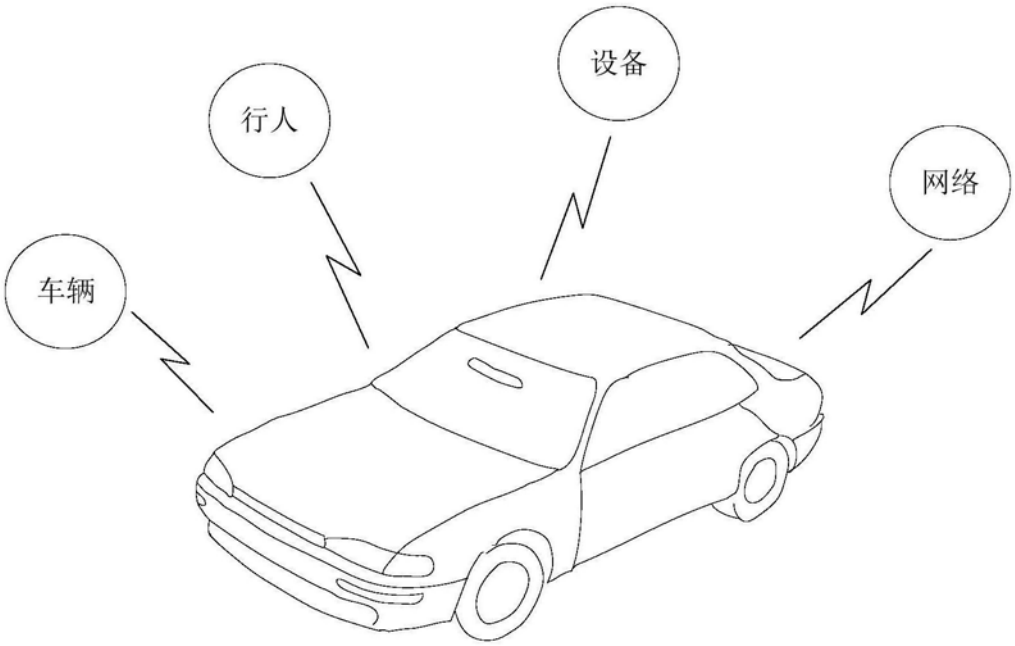

设备
行人
网络
车辆

图1

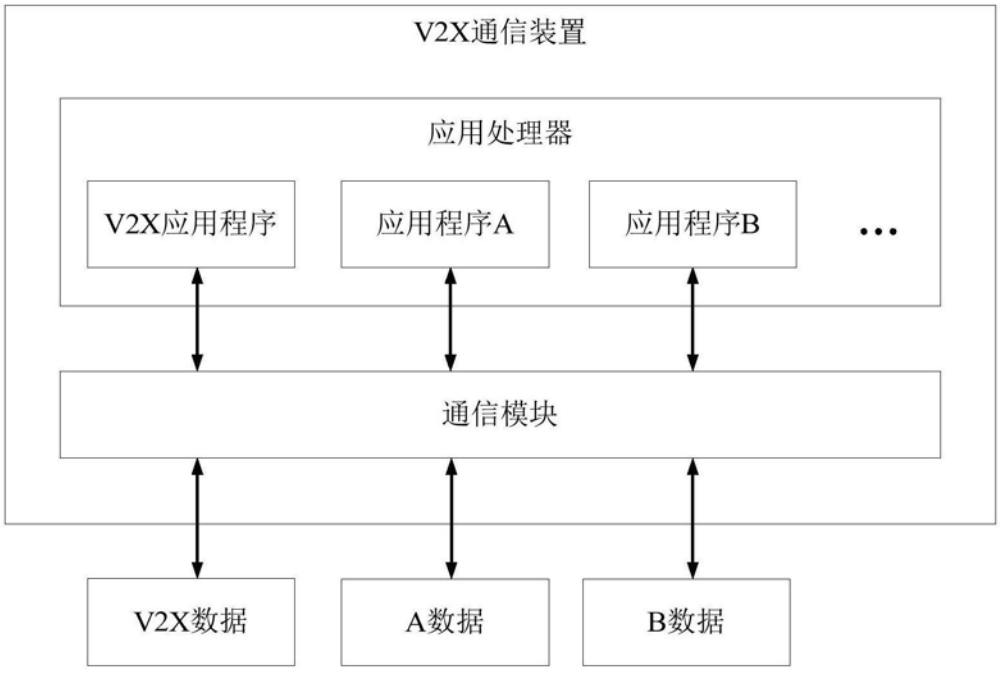

V2X通信装置
应用处理器
V2X应用程序
应用程序A
应用程序B
...
通信模块
V2X数据
A数据
B数据

图2

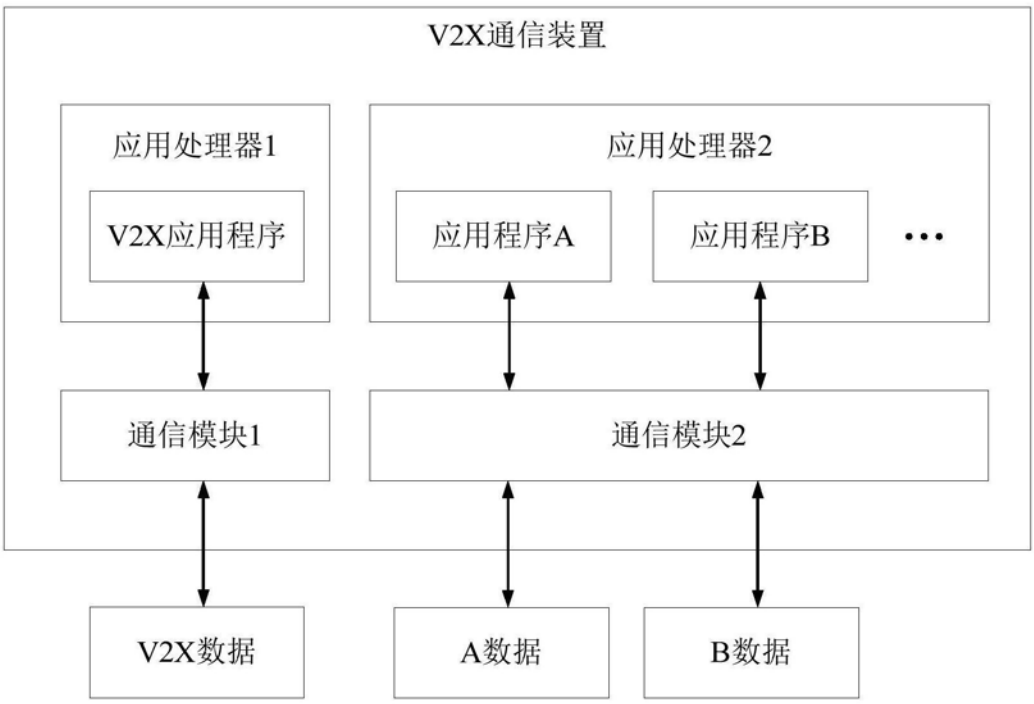

V2X通信装置
应用处理器1
V2X应用程序
应用处理器2
应用程序A
应用程序B
•••
通信模块1
通信模块2
V2X数据
A数据
B数据

图3

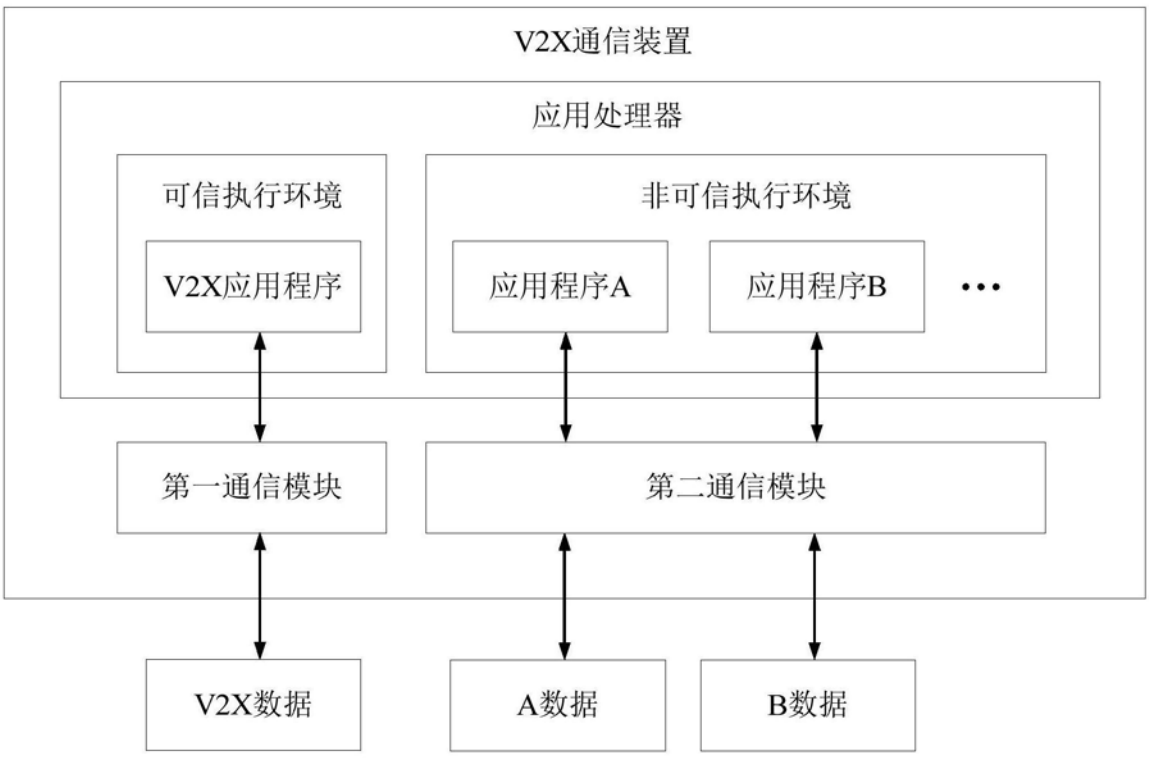

V2X通信装置
应用处理器
可信执行环境
V2X应用程序
非可信执行环境
应用程序A
应用程序B
•••
第一通信模块
第二通信模块
V2X数据
A数据
B数据

图4

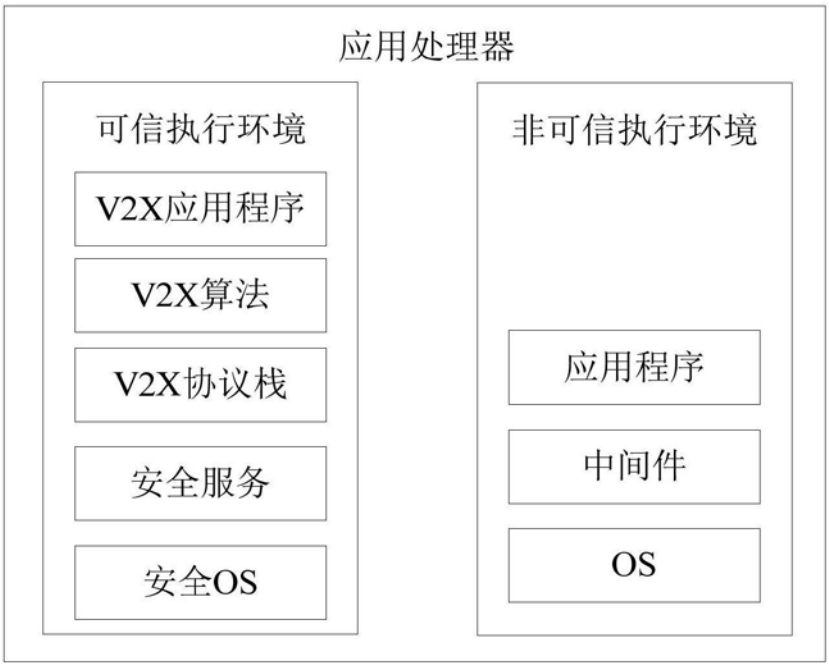

应用处理器
可信执行环境
V2X应用程序
V2X算法
V2X协议栈
安全服务
安全OS
非可信执行环境
应用程序
中间件
OS

图5

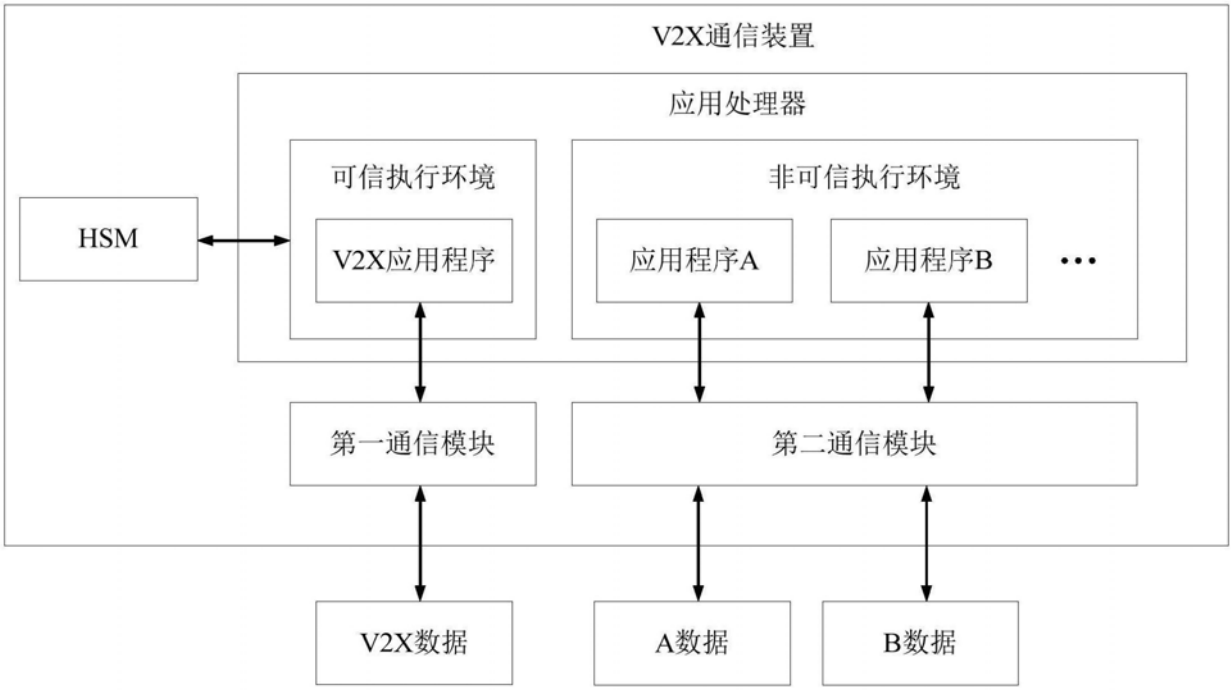

V2X通信装置
应用处理器
可信执行环境
非可信执行环境
HSM
V2X应用程序
应用程序A
应用程序B
•••
第一通信模块
第二通信模块
V2X数据
A数据
B数据

图6

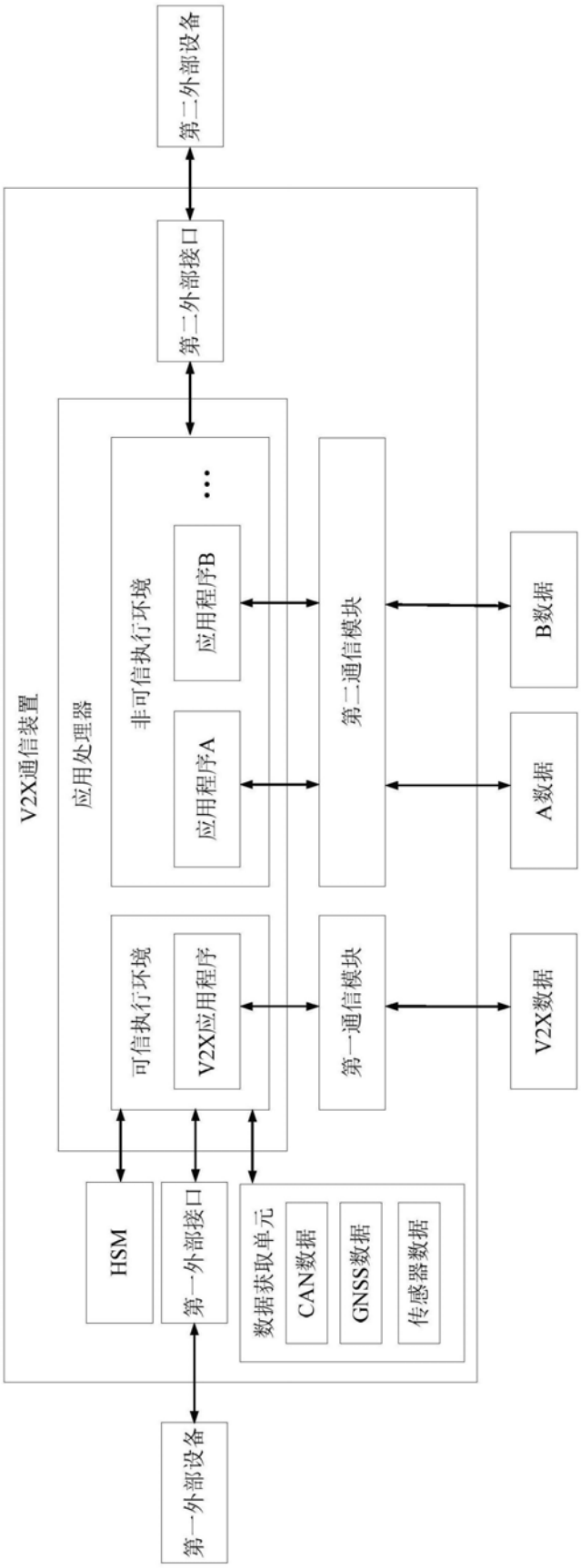

第二外部设备
第二外部接口
V2X通信装置
应用处理器
非可信执行环境
应用程序B
...
应用程序A
第二通信模块
B数据
A数据
可信执行环境
V2X应用程序
第一通信模块
V2X数据
HSM
第一外部接口
数据获取单元
CAN数据
GNSS数据
传感器数据
第一外部设备

图7

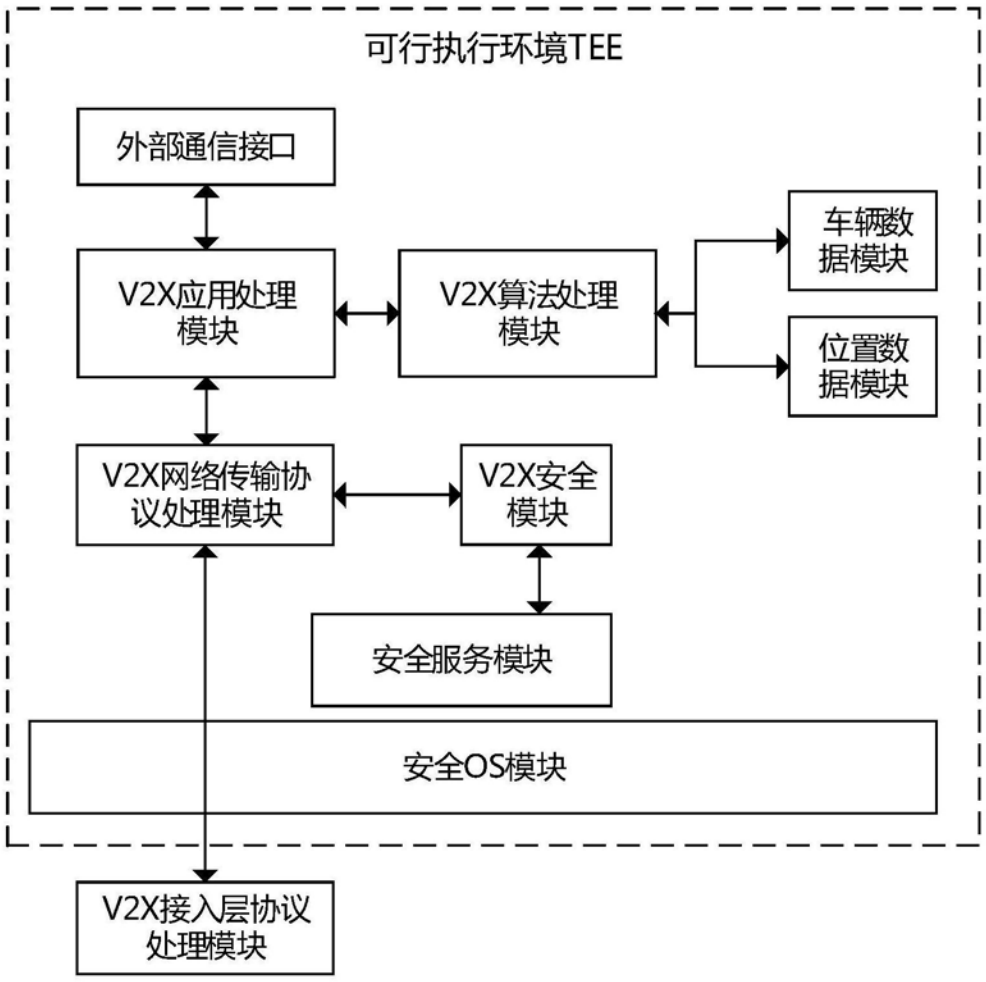

可行执行环境TEE
外部通信接口
V2X应用处理模块
V2X算法处理模块
车辆数据模块
位置数据模块
V2X网络传输协议处理模块
V2X安全模块
安全服务模块
安全OS模块
V2X接入层协议处理模块

图8

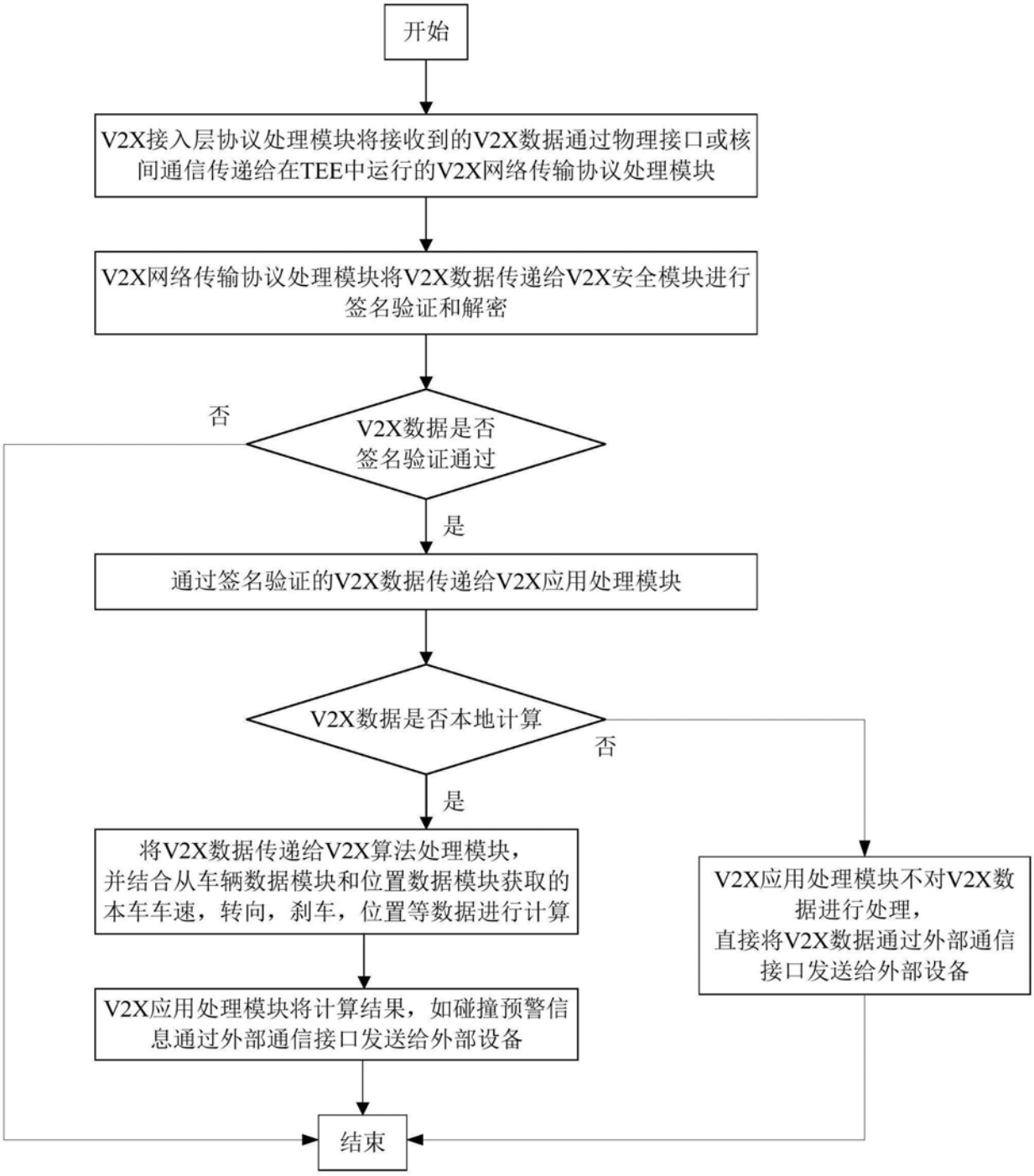

开始
V2X接入层协议处理模块将接收到的V2X数据通过物理接口或核间通信传递给在TEE中运行的V2X网络传输协议处理模块
V2X网络传输协议处理模块将V2X数据传递给V2X安全模块进行签名验证和解密
否
V2X数据是否签名验证通过
是
通过签名验证的V2X数据传递给V2X应用处理模块
V2X数据是否本地计算
否
是
将V2X数据传递给V2X算法处理模块，并结合从车辆数据模块和位置数据模块获取的本车车速，转向，刹车，位置等数据进行计算
V2X应用处理模块将计算结果，如碰撞预警信息通过外部通信接口发送给外部设备
V2X应用处理模块不对V2X数据进行处理，直接将V2X数据通过外部通信接口发送给外部设备
结束

图9

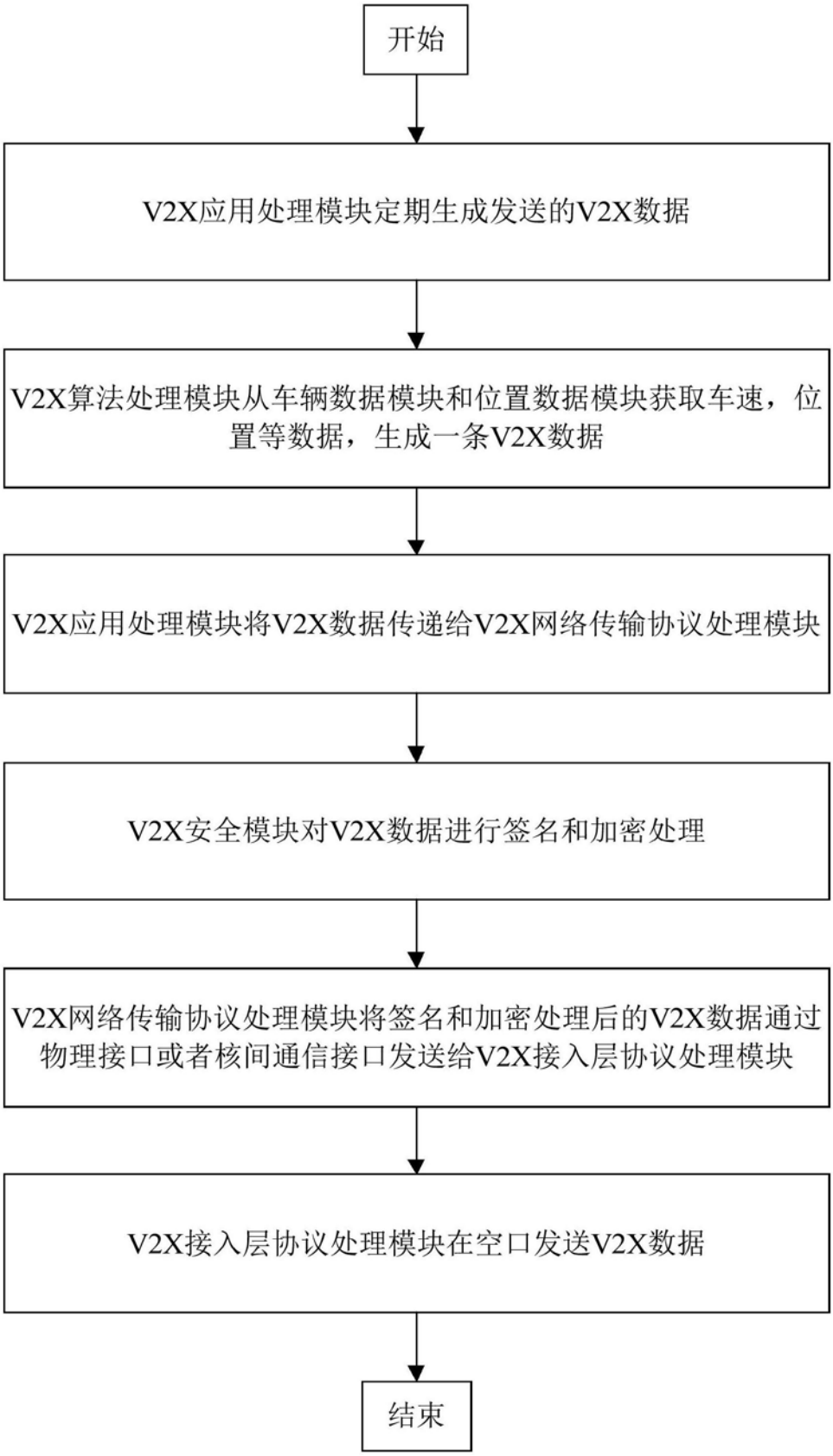

开始
V2X应用处理模块定期生成发送的V2X数据
V2X算法处理模块从车辆数据模块和位置数据模块获取车速，位置等数据，生成一条V2X数据
V2X应用处理模块将V2X数据传递给V2X网络传输协议处理模块
V2X安全模块对V2X数据进行签名和加密处理
V2X网络传输协议处理模块将签名和加密处理后的V2X数据通过物理接口或者核间通信接口发送给V2X接入层协议处理模块
V2X接入层协议处理模块在空口发送V2X数据
结束

图10

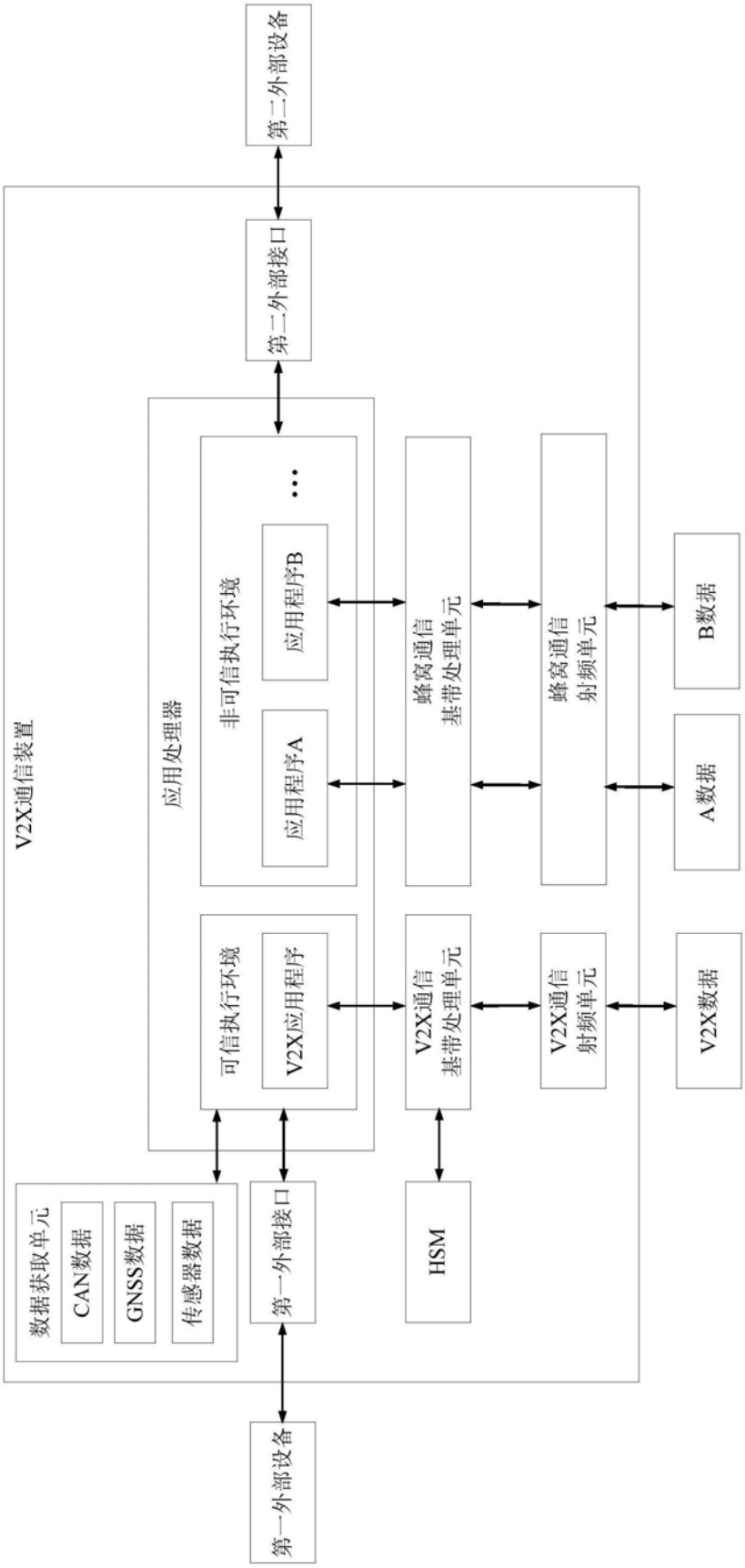

第二外部设备
第二外部接口
V2X通信装置
应用处理器
非可信执行环境
应用程序B
应用程序A
...
蜂窝通信
基带处理单元
蜂窝通信
射频单元
B数据
A数据
可信执行环境
V2X应用程序
V2X通信
基带处理单元
V2X通信
射频单元
V2X数据
数据获取单元
CAN数据
GNSS数据
传感器数据
第一外部接口
HSM
第一外部设备

图11

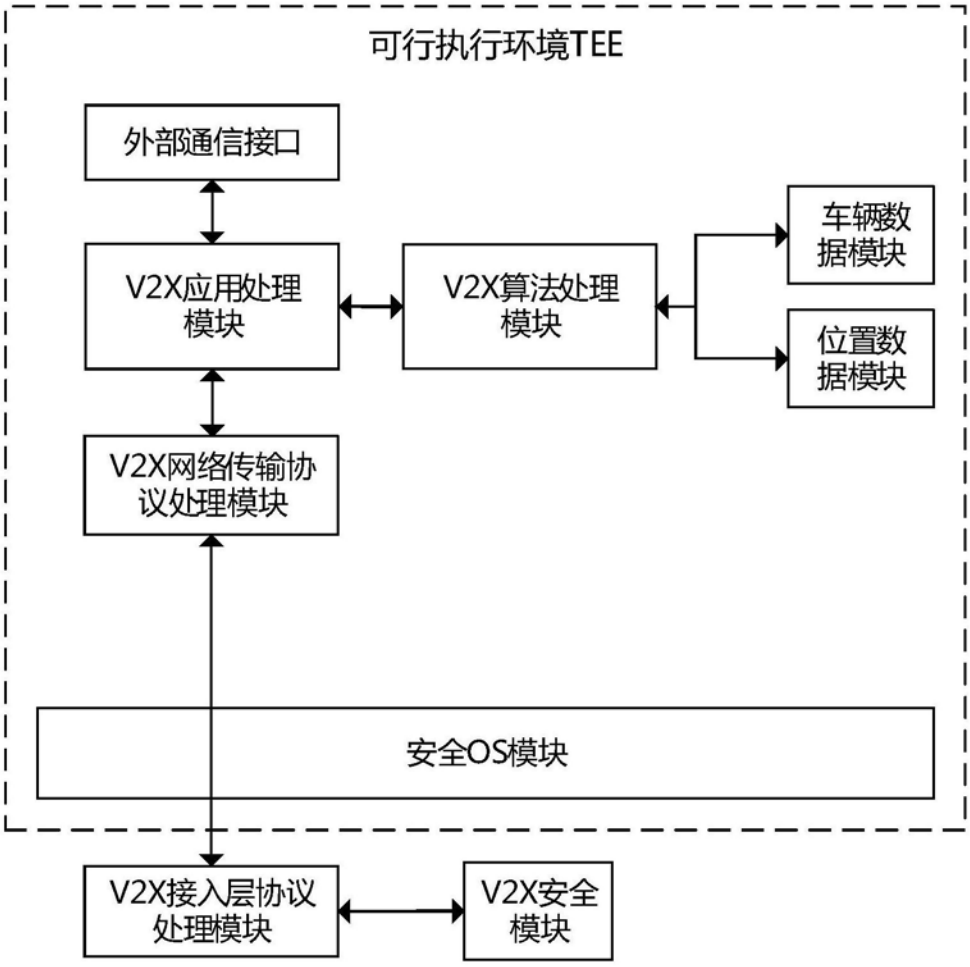

可行执行环境TEE
外部通信接口
V2X应用处理模块
V2X算法处理模块
车辆数据模块
位置数据模块
V2X网络传输协议处理模块
安全OS模块
V2X接入层协议处理模块
V2X安全模块

图12

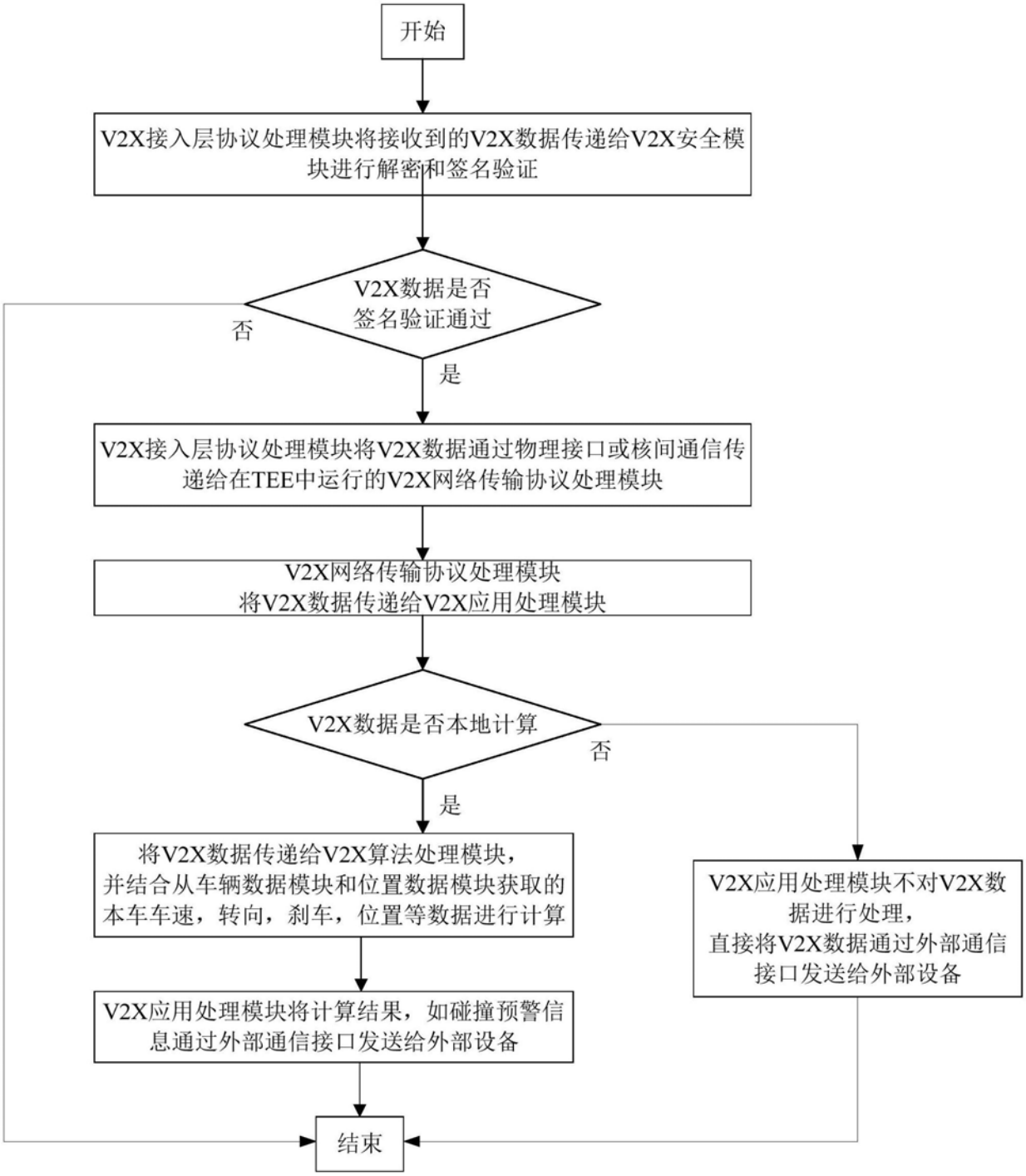

开始
V2X接入层协议处理模块将接收到的V2X数据传递给V2X安全模块进行解密和签名验证
V2X数据是否签名验证通过
否
是
V2X接入层协议处理模块将V2X数据通过物理接口或核间通信传递给在TEE中运行的V2X网络传输协议处理模块
V2X网络传输协议处理模块将V2X数据传递给V2X应用处理模块
V2X数据是否本地计算
否
是
将V2X数据传递给V2X算法处理模块，并结合从车辆数据模块和位置数据模块获取的本车车速，转向，刹车，位置等数据进行计算
V2X应用处理模块将计算结果，如碰撞预警信息通过外部通信接口发送给外部设备
V2X应用处理模块不对V2X数据进行处理，直接将V2X数据通过外部通信接口发送给外部设备
结束

图13

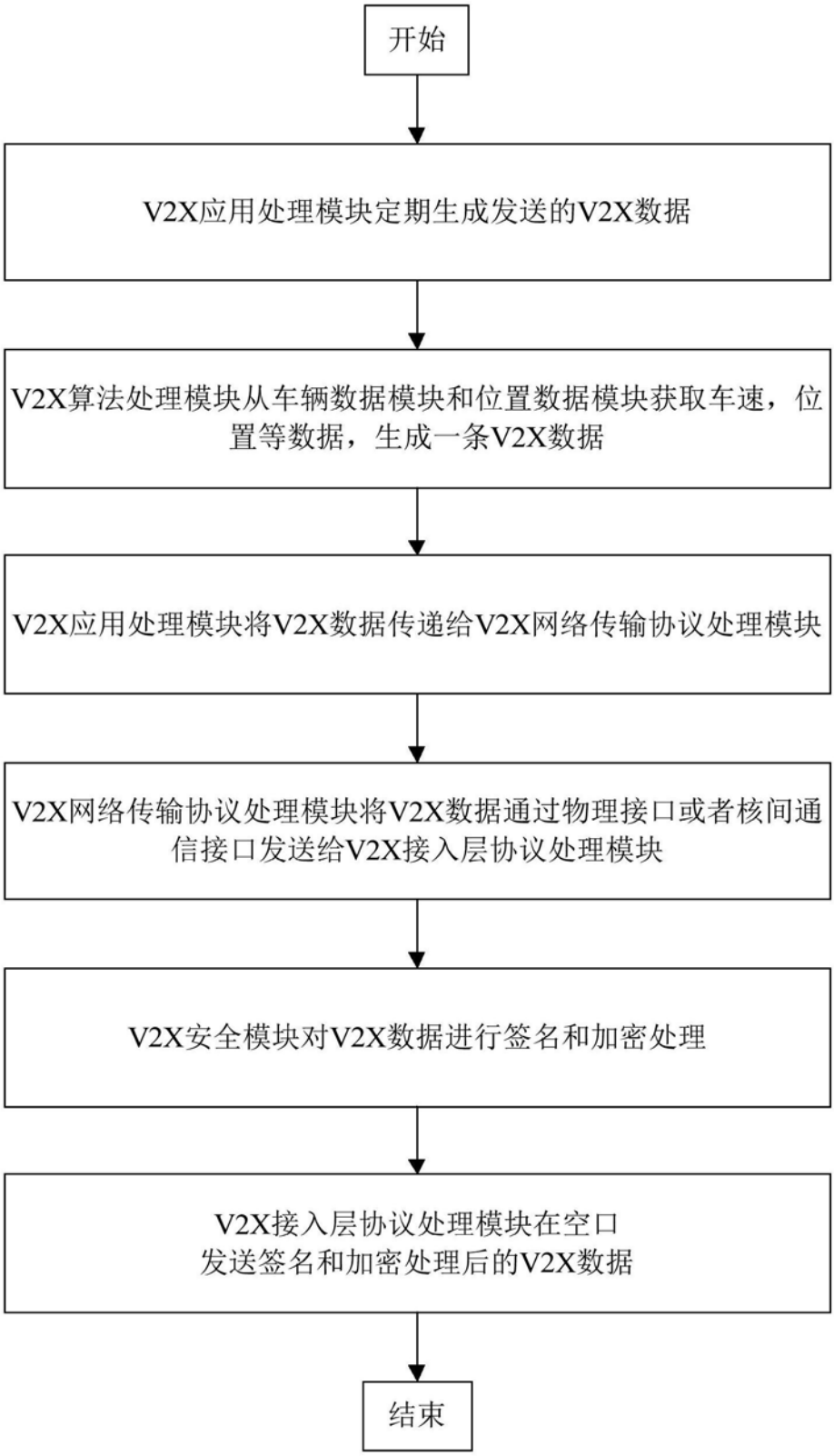

开始
V2X应用处理模块定期生成发送的V2X数据
V2X算法处理模块从车辆数据模块和位置数据模块获取车速，位置等数据，生成一条V2X数据
V2X应用处理模块将V2X数据传递给V2X网络传输协议处理模块
V2X网络传输协议处理模块将V2X数据通过物理接口或者核间通信接口发送给V2X接入层协议处理模块
V2X安全模块对V2X数据进行签名和加密处理
V2X接入层协议处理模块在空口
发送签名和加密处理后的V2X数据
结束

图14