(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 110149611 B
(45)授权公告日 2021.02.09

(21)申请号 201910320383.3
(22)申请日 2019.04.19
(65)同一申请的已公布的文献号
申请公布号 CN 110149611 A
(43)申请公布日 2019.08.20
(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 张浩 胡歌华
(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健
(51)Int.Cl.
H04W 4/40(2018.01)
H04W 12/00(2009.01)
H04W 12/02(2009.01)

审查员 段巍巍

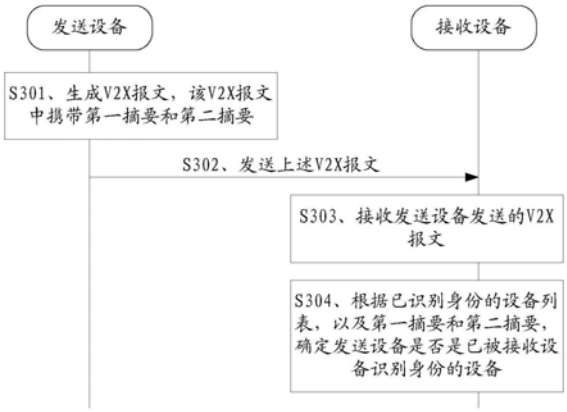
权利要求书4页 说明书22页 附图6页

(54)发明名称

一种身份验证方法、设备、系统及计算机可读介质

(57)摘要

本申请公开了一种身份验证方法、设备、系统及计算机可读介质，涉及通信领域。该方法应用于设备进行V2X通信中时，可在不增加处理时延和消息验证负担的同时，提升了网络信息的安全性。接收设备接收发送设备发送的携带第一摘要和第二摘要的V2X报文，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的MAC地址的摘要；接收设备根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备，如果接收设备确定出发送设备不是已被自身识别身份的设备，可认为该V2X报文中的数据是不可信任的。如果接收设备确定出发送设备是已被自身识别身份的设备，可认为该V2X报文中的数据是可信任的。



CN 110149611 B

1.一种身份验证方法,其特征在于,包括:

接收设备接收发送设备发送的车辆与其他设备通信V2X报文,所述V2X报文中携带第一摘要和第二摘要,所述第一摘要是所述发送设备的身份信息的摘要,所述第二摘要是所述发送设备的媒体访问控制MAC地址的摘要;

所述接收设备根据已识别身份的设备列表,以及所述第一摘要和所述第二摘要,确定所述发送设备是否是已被所述接收设备识别身份的设备;

如果所述已识别身份的设备列表中未包括所述第一摘要和/或所述第二摘要,则所述接收设备确定所述发送设备未被所述接收设备识别身份;

所述接收设备获取所述发送设备的身份信息和所述发送设备的MAC地址;

所述接收设备利用消息摘要算法分别确定所述发送设备的身份信息的摘要和所述发送设备的MAC地址的摘要;

所述接收设备在确定所述第一摘要与确定出的所述发送设备的身份信息的摘要相同,且所述第二摘要与确定出的所述发送设备的MAC地址的摘要相同时,将所述第一摘要和所述第二摘要存储在所述已识别身份的设备列表中。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

如果所述已识别身份的设备列表中包括所述第一摘要和所述第二摘要,则所述接收设备确定所述发送设备是已被所述接收设备识别身份的设备;

所述接收设备确定所述V2X报文中的数据是可信任数据。

3.根据权利要求1或2所述的方法,其特征在于,所述接收设备获取所述发送设备的身份信息和所述发送设备的MAC地址,包括:

所述接收设备向发送设备发送身份请求报文,所述身份请求报文中携带所述第一摘要和所述第二摘要;

所述接收设备接收所述发送设备发送的身份响应报文,所述身份响应报文中携带加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址;

所述接收设备分别对加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址进行解密,获得所述发送设备的身份信息和所述发送设备的MAC地址。

4.根据权利要求1所述的方法,其特征在于,在所述接收设备获取所述发送设备的身份信息和所述发送设备的MAC地址之后,所述方法还包括:

所述接收设备确定获取到的所述发送设备的MAC地址与所述V2X报文中携带的MAC地址一致。

5.根据权利要求1所述的方法,其特征在于,在所述将所述第一摘要和所述第二摘要存储在所述已识别身份的设备列表中之后,所述方法还包括:

所述接收设备在第一时长后从所述已识别身份的设备列表中删除所述第一摘要和所述第二摘要。

6.根据权利要求1所述的方法,其特征在于,在所述接收设备根据已识别身份的设备列表,以及所述第一摘要和所述第二摘要,确定所述发送设备是否是已被所述接收设备识别身份的设备之前,还包括:

所述接收设备利用消息摘要算法确定所述V2X报文中携带的MAC地址的摘要;

所述接收设备确定所述第二摘要与确定出的所述V2X报文中携带的MAC地址的摘要相

同。

7.根据权利要求2所述的方法,其特征在于,所述V2X报文中还携带第三摘要,所述第三摘要是所述发送设备的隐私信息的摘要;

所述接收设备确定所述V2X报文中的数据是可信任数据,包括:

所述接收设备在确定所述已识别身份的设备列表中包括所述第三摘要时,确定所述第三摘要是可信任数据。

8.根据权利要求7所述的方法,其特征在于,所述方法还包括:

如果所述接收设备确定所述已识别身份的设备列表中未包括所述第三摘要,则所述接收设备获取所述发送设备的隐私信息;

所述接收设备利用消息摘要算法确定所述发送设备的隐私信息的摘要;

所述接收设备在确定所述第三摘要与确定出的所述发送设备的隐私信息的摘要相同时,将所述第三摘要存储在所述已识别身份的设备列表中。

9.一种身份验证方法,其特征在于,所述方法包括:

发送设备生成车辆与其他设备通信V2X报文,所述V2X报文中携带第一摘要和第二摘要,所述第一摘要是所述发送设备的身份信息的摘要,所述第二摘要是所述发送设备的媒体访问控制MAC地址的摘要;

所述发送设备发送所述V2X报文;

所述发送设备接收身份请求报文,所述身份请求报文中携带所述第一摘要和所述第二摘要;

所述发送设备发送身份响应报文,所述身份响应报文中携带加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址。

10.根据权利要求9所述的方法,其特征在于,所述发送设备生成车辆与其他设备通信V2X报文,包括:

所述发送设备利用消息摘要算法确定所述发送设备的身份信息的摘要,以获得所述第一摘要;

所述发送设备利用消息摘要算法确定所述发送设备的MAC地址的摘要,以获得所述第二摘要;

所述发送设备生成所述V2X报文,所述V2X报文中携带所述第一摘要和所述第二摘要。

11.根据权利要求9或10所述的方法,其特征在于,所述V2X报文中还携带第三摘要;

所述方法还包括:所述发送设备利用所述消息摘要算法确定所述发送设备的隐私信息的摘要,以获得所述第三摘要。

12.一种接收设备,其特征在于,包括:处理器、存储器和移动通信模块;所述处理器、所述移动通信模块和所述存储器耦合,所述存储器用于存储计算机程序,当所述计算机程序被所述接收设备执行时,使得所述接收设备执行如下操作:

接收发送设备发送的车辆与其他设备通信V2X报文,所述V2X报文中携带第一摘要和第二摘要,所述第一摘要是所述发送设备的身份信息的摘要,所述第二摘要是所述发送设备的媒体访问控制MAC地址的摘要;

根据已识别身份的设备列表,以及所述第一摘要和所述第二摘要,确定所述发送设备是否是已被所述接收设备识别身份的设备;如果所述已识别身份的设备列表中未包括所述

第一摘要和/或所述第二摘要，则确定所述发送设备未被所述接收设备识别身份；获取所述发送设备的身份信息和所述发送设备的MAC地址；利用消息摘要算法分别确定所述发送设备的身份信息的摘要和所述发送设备的MAC地址的摘要；

在确定所述第一摘要与确定出的所述发送设备的身份信息的摘要相同，且所述第二摘要与确定出的所述发送设备的MAC地址的摘要相同时，将所述第一摘要和所述第二摘要存储在所述已识别身份的设备列表中。

13.根据权利要求12所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

如果所述已识别身份的设备列表中包括所述第一摘要和所述第二摘要，则确定所述发送设备是已被所述接收设备识别身份的设备；确定所述V2X报文中的数据是可信任数据。

14.根据权利要求12或13所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

发送身份请求报文，所述身份请求报文中携带所述第一摘要和所述第二摘要；接收所述发送设备发送的身份响应报文，所述身份响应报文中携带加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址；

分别对加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址进行解密，获得所述发送设备的身份信息和所述发送设备的MAC地址。

15.根据权利要求12所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

确定获取到的所述发送设备的MAC地址与所述V2X报文中携带的MAC地址一致。

16.根据权利要求12所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

在第一时长后从所述已识别身份的设备列表中删除所述第一摘要和所述第二摘要。

17.根据权利要求12所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

利用消息摘要算法确定所述V2X报文中携带的MAC地址的摘要；确定所述第二摘要与确定出的所述V2X报文中携带的MAC地址的摘要相同。

18.根据权利要求13所述的接收设备，其特征在于，所述V2X报文中还携带第三摘要，所述第三摘要是所述发送设备的隐私信息的摘要；

当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

在确定所述已识别身份的设备列表中包括所述第三摘要时，确定所述第三摘要是可信任数据。

19.根据权利要求18所述的接收设备，其特征在于，当所述计算机程序被所述接收设备执行时，还使得所述接收设备执行如下操作：

如果确定所述已识别身份的设备列表中未包括所述第三摘要，则获取所述发送设备的隐私信息；利用消息摘要算法确定所述发送设备的隐私信息的摘要；

在确定所述第三摘要与确定出的所述发送设备的隐私信息的摘要相同时，将所述第三摘要存储在所述已识别身份的设备列表中。

20.一种发送设备，其特征在于，包括：处理器、存储器和移动通信模块；所述处理器、所

述移动通信模块和所述存储器耦合，所述存储器用于存储计算机程序，当所述计算机程序被所述发送设备执行时，使得所述发送设备执行如下操作：

生成车辆与其他设备通信V2X报文，所述V2X报文中携带第一摘要和第二摘要，所述第一摘要是所述发送设备的身份信息的摘要，所述第二摘要是所述发送设备的媒体访问控制MAC地址的摘要；

发送所述V2X报文；接收身份请求报文，所述身份请求报文中携带所述第一摘要和所述第二摘要；发送身份响应报文，所述身份响应报文中携带加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址。

21.根据权利要求20所述的发送设备，其特征在于，当所述计算机程序被所述发送设备执行时，还使得所述发送设备执行如下操作：

利用消息摘要算法确定所述发送设备的身份信息的摘要，以获得所述第一摘要；利用消息摘要算法确定所述发送设备的MAC地址的摘要，以获得所述第二摘要；生成所述V2X报文，所述V2X报文中携带所述第一摘要和所述第二摘要。

22.根据权利要求20或21所述的发送设备，其特征在于，所述V2X报文中还携带第三摘要；

当所述计算机程序被所述发送设备执行时，还使得所述发送设备执行如下操作：利用所述消息摘要算法确定所述发送设备的隐私信息的摘要，以获得所述第三摘要。

23.一种信息处理装置，其特征在于，包括处理器，用于与存储器相连，调用所述存储器中存储的程序，以执行如权利要求1至11中任一项所述的身份验证方法。

24.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有一个或多个程序；

当所述计算机软件程序在信息处理装置中运行时，使得所述信息处理装置执行如权利要求1至11中任一项所述的身份验证方法。

25.一种通信系统，其特征在于，包括：如权利要求12-19中任一项所述的接收设备，以及如权利要求20-22中任一项所述的发送设备。

一种身份验证方法、设备、系统及计算机可读介质

技术领域

[0001] 本申请涉及通信领域，尤其涉及一种身份验证方法、设备及系统。

背景技术

[0002] 随着社会的不断发展，汽车越来越普及。车联网技术的兴起，使得车辆也越来越智能，越来越多的车辆使用车辆与其他设备通信(vehicleto everything，V2X)来传输车辆数据，以感知周边车辆的存在，并实现和周边车辆的直接交互，如碰撞报警，行人告警等。

[0003] 目前，V2X定义的车辆数据在传输时会包含一些敏感数据，如车辆身份信息等。这些敏感数据在当前规范中并没有要求要使用密文进行传输。考虑到使用密文传输时接收方还需要对消息进行解密，因此，目前多数厂商的设备(如车辆)在进行V2X通信时，车辆数据部分都是使用明文进行传输的。而采用明文传输车辆数据会存在信息安全隐患。不法分子很容易便能收集到一些车辆的敏感数据，如车辆身份信息，而后利用收集到的敏感数据进行不法活动。如不法分子获得某些车辆的车辆身份信息后通过仿冒车辆身份进行非法活动。且随着V2X的逐渐深入，会有越来越多的车辆数据被直接共享到路面上，这会带来越来越多的信息安全隐患。

[0004] 为了提升车辆身份信息等敏感数据的安全性，当前有些厂商使用自主私有协议约定利用对称加密算法使用密文来传输车辆数据。这种做法虽然解决了网络信息安全的问题，但如果所有车辆都使用这种做法来传输车辆数据，那么意味着接收方需要对接收到的每个车辆数据都进行验证。据估算，在道路拥堵的情况下，如果车辆都能够进行V2X通信，则每辆车在每秒中接收到的加密数据可能是一个庞大的数字，可能多达两千条以上，消息的解密必然会带来处理时延以及严重的消息验证负担。

[0005] 因此，在V2X通信时，如何在不增加处理时延和消息验证负担的同时，能够提升网络信息的安全性，已成为本领域技术人员研究的重点课题。

发明内容

[0006] 本申请实施例提供一种身份验证方法、设备及系统，V2X通信时在不增加处理时延和消息验证负担的同时，提升了网络信息的安全性。

[0007] 第一方面，本申请实施例提供一种身份验证方法，包括：

[0008] 接收设备接收发送设备发送的携带有第一摘要和第二摘要的V2X报文，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的媒体访问控制(mediaaccess control，MAC)地址的摘要；接收设备根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备；如果已识别身份的设备列表中未包括第一摘要和/或第二摘要，则接收设备可以认为发送设备未被接收设备识别身份；此时，接收设备可以获取发送设备的身份信息和发送设备的MAC地址，并利用消息摘要算法分别确定发送设备的身份信息的摘要和发送设备的MAC地址的摘要；在确定第一摘要与确定出的发送设备的身份信息的摘要相同，且第二摘要与确定出的发送设备的MAC地址的摘要

相同时，接收设备可以将第一摘要和第二摘要存储在上述已识别身份的设备列表中。

[0009] 采用上述技术方案，通过将V2X报文中目前规定需携带的身份信息隐式化，也就是说，采用由身份信息确定的摘要和由MAC地址确定的摘要替代，不以明文形式传送，从而达到接收设备与发送设备在进行V2V通信过程中，全程没有暴露车辆的身份信息。提高了身份信息传输的安全性。另外，对于接收设备来说，如果确定出发送方的身份没有被自身确认，则可以对接收到的包含该隐式化敏感数据的V2X报文进行验证来确认发送方的身份，并在确认后将隐式数据存储，以便后续不再对发送方的数据进行复杂的验证，而是通过对比存储的隐式数据来确认发送方的身份。这样，大大减轻了消息验证负担，缩短了处理时延。

[0010] 结合第一方面，在一种可能的实现方式中，该方法还包括：如果已识别身份的设备列表中包括第一摘要和第二摘要，则接收设备可确定发送设备是已被接收设备识别身份的设备；此时，接收设备可以确定V2X报文中的数据是可信任数据，从而可利用V2X报文中的数据进行相关处理。

[0011] 结合第一方面和上述可能的实现方式，在另一种可能的实现方式中，上述接收设备获取发送设备的身份信息和发送设备的MAC地址，具体的可以包括：接收设备发送携带第一摘要和第二摘要的身份请求报文；接收设备接收发送设备发送的身份响应报文，该身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址；接收设备分别对加密的发送设备的身份信息和加密的发送设备的MAC地址进行解密，以获得发送设备的身份信息和发送设备的MAC地址。通过交互加密的身份信息和加密的MAC地址，以便接收设备获得发送设备的身份信息和MAC地址。另外，由于恶意的设备无法获得加密密钥，因此，也就无法获得发送设备的真实身份信息和MAC地址，进一步的提高了身份信息传输的安全性。

[0012] 结合第一方面和上述可能的实现方式，在另一种可能的实现方式中，在上述接收设备获取发送设备的身份信息和发送设备的MAC地址之后，该方法还可以包括：接收设备可以判断获取到的发送设备的MAC地址与V2X报文中携带的MAC地址是否一致，如果两者一致，则进行发送设备的身份验证过程；如果两者不一致，则可直接丢弃报文。这样，可以降低接收设备的验证负担。

[0013] 结合第一方面和上述可能的实现方式，在另一种可能的实现方式中，在上述将第一摘要和第二摘要存储在已识别身份的设备列表中之后，该方法还可以包括：接收设备在第一时长后从已识别身份的设备列表中删除第一摘要和第二摘要。这样，可进一步提高信息的安全性。

[0014] 结合第一方面和上述可能的实现方式，在另一种可能的实现方式中，在上述接收设备根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备之前，该方法还可以包括：接收设备利用消息摘要算法确定V2X报文中携带的MAC地址的摘要；接收设备可先判断第二摘要与确定出的V2X报文中携带的MAC地址的摘要是否相同。如果第二摘要与确定出的V2X报文中携带的MAC地址的摘要相同，则可执行根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备的操作。如果第二摘要与确定出的V2X报文中携带的MAC地址的摘要不同，则可丢弃接收到的报文。这样，可降低接收设备的验证负担。

[0015] 结合第一方面和上述可能的实现方式，在另一种可能的实现方式中，上述V2X报文中还可以携带第三摘要，该第三摘要是发送设备的隐私信息的摘要；如，隐私信息可以包括

发送设备的尺寸信息,发送设备的类型(如车辆类型)等。上述接收设备确定V2X报文中的数据是可信任数据,具体的可以包括:接收设备在确定已识别身份的设备列表中包括第三摘要时,确定第三摘要是可信任数据。这样,通过对这些隐私信息用密文代替明文传输,可以确保其传输的安全性。

[0016] 结合第一方面和上述可能的实现方式,在另一种可能的实现方式中,该方法还可以包括:如果接收设备确定已识别身份的设备列表中未包括第三摘要,则接收设备获取发送设备的隐私信息;接收设备利用消息摘要算法确定发送设备的隐私信息的摘要;接收设备在确定第三摘要与确定出的发送设备的隐私信息的摘要相同时,将第三摘要存储在已识别身份的设备列表中。这样,通过在确认第三摘要是可信任数据后将其存储,以便后续不再对该数据进行复杂的验证,而是通过对比存储的数据便可确认其是否可信任。这样,进一步减轻了消息验证负担,缩短了处理时延。

[0017] 第二方面,本申请实施例提供一种身份验证方法,该方法可以包括:发送设备生成并发送V2X报文,该V2X报文中携带第一摘要和第二摘要,第一摘要是发送设备的身份信息的摘要,第二摘要是发送设备的媒体访问控制MAC地址的摘要;发送设备接收携带第一摘要和第二摘要的身份请求报文,并发送身份响应报文,该身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址。

[0018] 采用上述技术方案,通过将V2X报文中目前规定需携带的身份信息隐式化,也就是说,采用由身份信息确定的摘要和由MAC地址确定的摘要替代,不以明文形式传送,从而达到接收设备与发送设备在进行V2V通信过程中,全程没有暴露车辆的身份信息。提高了身份信息传输的安全性。

[0019] 结合第二方面,在一种可能的实现方式中,发送设备生成车辆与其他设备通信V2X报文,具体的可以包括:发送设备利用消息摘要算法确定发送设备的身份信息的摘要,以获得第一摘要,利用消息摘要算法确定发送设备的MAC地址的摘要,以获得第二摘要,生成携带第一摘要和第二摘要的V2X报文。

[0020] 结合第二方面和上述可能的实现方式,在另一种可能的实现方式中,上述V2X报文中还可以携带第三摘要;该方法还可以包括:发送设备利用消息摘要算法确定发送设备的隐私信息的摘要,以获得第三摘要。这样,通过对隐私信息用密文代替明文传输,可以确保其传输的安全性。

[0021] 第三方面,本申请实施例提供一种接收设备,该接收设备可以包括:处理器、存储器和移动通信模块;处理器、移动通信模块和存储器耦合,存储器用于存储计算机程序代码,计算机程序代码包括计算机指令,当该计算机指令被接收设备执行时,使得该接收设备执行如下操作:接收发送设备发送的V2X报文,V2X报文中携带第一摘要和第二摘要,第一摘要是发送设备的身份信息的摘要,第二摘要是发送设备的MAC地址的摘要;根据已识别身份的设备列表,以及第一摘要和第二摘要,确定发送设备是否是已被接收设备识别身份的设备;如果已识别身份的设备列表中未包括第一摘要和/或第二摘要,则确定发送设备未被接收设备识别身份;获取发送设备的身份信息和发送设备的MAC地址;利用消息摘要算法分别确定发送设备的身份信息的摘要和发送设备的MAC地址的摘要;在确定第一摘要与确定出的发送设备的身份信息的摘要相同,且第二摘要与确定出的发送设备的MAC地址的摘要相同时,将第一摘要和第二摘要存储在已识别身份的设备列表中。

[0022] 结合第三方面，在一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：如果已识别身份的设备列表中包括第一摘要和第二摘要，则确定发送设备是已被接收设备识别身份的设备；确定V2X报文中的数据是可信任数据。

[0023] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：发送身份请求报文，身份请求报文中携带第一摘要和第二摘要；接收发送设备发送的身份响应报文，身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址；分别对加密的发送设备的身份信息和加密的发送设备的MAC地址进行解密，获得发送设备的身份信息和发送设备的MAC地址。

[0024] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：确定获取到的发送设备的MAC地址与V2X报文中携带的MAC地址一致。

[0025] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：在第一时长后从已识别身份的设备列表中删除第一摘要和第二摘要。

[0026] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：利用消息摘要算法确定V2X报文中携带的MAC地址的摘要；确定第二摘要与确定出的V2X报文中携带的MAC地址的摘要相同。

[0027] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，V2X报文中还携带第三摘要，第三摘要是发送设备的隐私信息的摘要；当计算机指令被接收设备执行时，还使得接收设备执行如下操作：在确定已识别身份的设备列表中包括第三摘要时，确定第三摘要是可信任数据。

[0028] 结合第三方面或上述可能的实现方式，在另一种可能的实现方式中，当计算机指令被接收设备执行时，还使得接收设备执行如下操作：如果确定已识别身份的设备列表中未包括第三摘要，则获取发送设备的隐私信息；利用消息摘要算法确定发送设备的隐私信息的摘要；在确定第三摘要与确定出的发送设备的隐私信息的摘要相同时，将第三摘要存储在已识别身份的设备列表中。

[0029] 第四方面，本申请实施例提供一种发送设备，包括：处理器、存储器和移动通信模块；处理器、移动通信模块和存储器耦合，存储器用于存储计算机程序代码，计算机程序代码包括计算机指令，当计算机指令被发送设备执行时，使得发送设备执行如下操作：生成车辆与其他设备通信V2X报文，V2X报文中携带第一摘要和第二摘要，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的媒体访问控制MAC地址的摘要；发送V2X报文；接收身份请求报文，身份请求报文中携带第一摘要和第二摘要；发送身份响应报文，身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址。

[0030] 结合第四方面，在一种可能的实现方式中，当计算机指令被发送设备执行时，还使得发送设备执行如下操作：利用消息摘要算法确定发送设备的身份信息的摘要，以获得第一摘要；利用消息摘要算法确定发送设备的MAC地址的摘要，以获得第二摘要；生成V2X报文，V2X报文中携带第一摘要和第二摘要。

[0031] 结合第四方面或上述可能的实现方式，在另一种可能的实现方式中，V2X报文中还携带第三摘要；当计算机指令被发送设备执行时，还使得发送设备执行如下操作：利用消息

摘要算法确定发送设备的隐私信息的摘要，以获得第三摘要。

[0032] 第五方面，本申请实施例提供一种接收设备，该接收设备可以包括：接收单元，用于接收发送设备发送的V2X报文，V2X报文中携带第一摘要和第二摘要，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的MAC地址的摘要；确定单元，用于根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备；如果已识别身份的设备列表中未包括第一摘要和/或第二摘要，则确定发送设备未被接收设备识别身份；获取单元，用于获取发送设备的身份信息和发送设备的MAC地址；确定单元，还用于利用消息摘要算法分别确定发送设备的身份信息的摘要和发送设备的MAC地址的摘要；存储单元，用于在确定单元确定第一摘要与确定出的发送设备的身份信息的摘要相同，且第二摘要与确定出的发送设备的MAC地址的摘要相同时，将第一摘要和第二摘要存储在已识别身份的设备列表中。

[0033] 结合第五方面，在一种可能的实现方式中，确定单元，还用于如果已识别身份的设备列表中包括第一摘要和第二摘要，则确定发送设备是已被接收设备识别身份的设备；确定V2X报文中的数据是可信任数据。

[0034] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，接收设备，还可以包括：发送单元，用于发送身份请求报文，身份请求报文中携带第一摘要和第二摘要；接收单元，还用于接收发送设备发送的身份响应报文，身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址；获取单元，具体用于分别对加密的发送设备的身份信息和加密的发送设备的MAC地址进行解密，获得发送设备的身份信息和发送设备的MAC地址。

[0035] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，确定单元，还用于确定获取到的发送设备的MAC地址与V2X报文中携带的MAC地址一致。

[0036] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，存储单元，还用于在第一时长后从已识别身份的设备列表中删除第一摘要和第二摘要。

[0037] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，确定单元，还用于利用消息摘要算法确定V2X报文中携带的MAC地址的摘要；确定第二摘要与确定出的V2X报文中携带的MAC地址的摘要相同。

[0038] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，V2X报文中还携带第三摘要，第三摘要是发送设备的隐私信息的摘要；确定单元，具体用于在确定已识别身份的设备列表中包括第三摘要时，确定第三摘要是可信任数据。

[0039] 结合第五方面或上述可能的实现方式，在另一种可能的实现方式中，获取单元，还用于如果确定单元确定已识别身份的设备列表中未包括第三摘要，则获取发送设备的隐私信息；确定单元，还用于利用消息摘要算法确定发送设备的隐私信息的摘要；存储单元，还用于在确定单元确定第三摘要与确定出的发送设备的隐私信息的摘要相同时，将第三摘要存储在已识别身份的设备列表中。

[0040] 第六方面，本申请实施例提供一种发送设备，包括：生成单元，用于生成V2X报文，V2X报文中携带第一摘要和第二摘要，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的媒体访问控制MAC地址的摘要；发送单元，用于发送V2X报文；接收单元，用于接收身份请求报文，身份请求报文中携带第一摘要和第二摘要；发送单元，还用于发送身份响

应报文,身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址。

[0041] 结合第六方面,在一种可能的实现方式中,生成单元,具体用于利用消息摘要算法确定发送设备的身份信息的摘要,以获得第一摘要;利用消息摘要算法确定发送设备的MAC地址的摘要,以获得第二摘要;生成V2X报文,V2X报文中携带第一摘要和第二摘要。

[0042] 结合第六方面或上述可能的实现方式,在另一种可能的实现方式中,V2X报文中还携带第三摘要;生成单元,还用于利用消息摘要算法确定发送设备的隐私信息的摘要,以获得第三摘要。

[0043] 第七方面,本申请实施例提供一种信息处理装置,该信息处理装置可以包括处理器,用于与存储器相连,调用存储器中存储的程序,以执行如第一方面或第一方面的可能的实现方式中任一所述的身份验证方法,或者,执行如第二方面或第二方面的可能的实现方式中任一所述的身份验证方法。

[0044] 第八方面,本申请实施例提供一种计算机可读存储介质,包括:计算机软件指令;当计算机软件指令在信息处理装置中运行时,使得信息处理装置执行如第一方面或第一方面的可能的实现方式中任一所述的身份验证方法,或者,执行如第二方面或第二方面的可能的实现方式中任一所述的身份验证方法。

[0045] 上述信息处理装置可以是本申请实施例中所述的信息处理系统,其可以包含在上述发送设备或接收设备中。

[0046] 第九方面,本申请实施例提供一种通信系统,该通信系统可以包括:如第三方面或第三方面的可能的实现方式,或第五方面或第五方面的可能的实现方式中任一所述的接收设备,以及如第四方面或第四方面的可能的实现方式,或第六方面或第六方面的可能的实现方式中任一所述的发送设备。

[0047] 其中,发送设备,用于生成V2X报文,该V2X报文中携带第一摘要和第二摘要,第一摘要是发送设备的身份信息的摘要,第二摘要是发送设备的MAC地址的摘要;发送该V2X报文。接收设备,用于接收发送设备发送的V2X报文;根据已识别身份的设备列表,以及第一摘要和第二摘要,确定发送设备是否是已被接收设备识别身份的设备;如果已识别身份的设备列表中未包括第一摘要和/或第二摘要,则确定发送设备未被接收设备识别身份;获取发送设备的身份信息和发送设备的MAC地址;利用消息摘要算法分别确定发送设备的身份信息的摘要和发送设备的MAC地址的摘要;在确定第一摘要与确定出的发送设备的身份信息的摘要相同,且第二摘要与确定出的发送设备的MAC地址的摘要相同时,将第一摘要和第二摘要存储在已识别身份的设备列表中。

[0048] 结合第九方面,在一种可能的实现方式中,接收设备,还用于如果已识别身份的设备列表中包括第一摘要和第二摘要,则确定发送设备是已被接收设备识别身份的设备,确定V2X报文中的数据是可信任数据。

[0049] 结合第九方面或上述可能的实现方式,在另一种可能的实现方式中,接收设备用于获取发送设备的身份信息和发送设备的MAC地址,包括:接收设备发送身份请求报文,身份请求报文中携带第一摘要和第二摘要,接收发送设备发送的身份响应报文,身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址,分别对加密的所述发送设备的身份信息和加密的所述发送设备的MAC地址进行解密,获得所述发送设备的身份信息和所述发送设备的MAC地址。发送设备,还用于接收身份请求报文,发送身份响应报文。

[0050] 可以理解地，上述提供的第三方面和第五方面所述的接收设备，上述提供的第四方面和第六方面所述的发送设备，上述提供的第七方面所述的信息处理装置，上述提供的第八方面所述的计算机可读存储介质，以及第九方面所述的通信系统均用于执行上文所提供的对应的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

附图说明

[0051] 图1为本申请实施例提供的一种系统架构的组成示意图；

[0052] 图2为本申请实施例提供的一种信息处理系统的结构示意图；

[0053] 图3为本申请实施例提供的一种身份验证方法的流程示意图；

[0054] 图4为本申请实施例提供的另一种身份验证方法的流程示意图；

[0055] 图5为本申请实施例提供的又一种身份验证方法的流程示意图；

[0056] 图6为本申请实施例提供的又一种身份验证方法的流程示意图；

[0057] 图7为本申请实施例提供的一种接收设备的组成示意图；

[0058] 图8为本申请实施例提供的一种发送设备的组成示意图。

具体实施方式

[0059] 以下，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

[0060] 为了在设备进行V2X通信时在不增加处理时延和消息验证负担的同时，提升车辆数据传输的安全性，本申请实施例提供一种身份验证方法，该方法可以将V2X报文(如基本安全消息(basic safety message，BSM)报文)中车辆数据包含的如车辆身份信息等敏感数据隐式化。也就是说，对于车辆数据包含的敏感数据不以明文形式传送，即对外不直接暴露，这样，可提高车辆数据传输的安全性。同时，对于接收方来说，仅在第一次接收到包含该隐式化敏感数据的V2X报文后需要通过验证过程来验证确认发送方的身份，后续不再对发送方的数据进行复杂的验证，而是通过对比存储的隐式数据来确认发送方的身份。这样，大大减轻了消息验证负担，缩短了处理时延。

[0061] 以下将结合附图，对本申请实施例中的技术方案进行描述。

[0062] 请参考图1，为本申请实施例提供的一种系统架构的组成示意图。如图1所示，该系统架构可以包括：发送设备101和接收设备102。

[0063] 发送设备101和接收设备102均具备V2X通信的能力。利用V2X(或C-V2X)，发送设备101和接收设备102可直接进行数据的交互。如，利用C-V2X，发送设备101和接收设备102可直接进行车辆数据的交互，以实现设备(如车辆)间的相互感知。

[0064] 其中，发送设备101和接收设备102具体的可以是利用各自包括的信息处理系统来实现V2X通信的。信息处理系统的具体结构可参考图2所示，以下实施例中将详细描述。

[0065] V2X英文全称为vehicle to everything，中文解释为车辆与其他设备通信，也可以称为车用无线通信技术。其是将车辆与一切事物相连接的新一代信息通信技术。C-V2X是

基于蜂窝(cellular)技术的V2X,它是基于第三代合作伙伴项目(the3rd generation partnershipproject,3GPP)全球统一标准的通信技术,或者说是基于3G/4G/5G等蜂窝网通信技术演进形成的车用无线通信技术。如,C-V2X可包含长期演进(long term evolution,LTE)-V2X和5G-V2X,从技术演进角度讲,LTE-V2X支持向5G-V2X平滑演进。本申请实施例提供的方法可适用于基于任何蜂窝(如3G/4G/5G,以及下一代的蜂窝网通信技术)技术的V2X。在另一些实施例中,本申请实施例提供的方法还可适用于基于无线保真(wireless fidelity,WIFI),通用串行总线(universal serial bus,USB)等技术的V2X。

[0066] 其中,V代表车辆,X代表任何与车辆交互信息的对象。当前X主要包含车辆、人(或说行人设备)、交通路侧基础设施(或称为路侧单元,其是设置在路边可实现V2X通信,支持V2X应用的硬件单元)和网络。

[0067] C-V2X(或V2X)概述的信息交互可以包括:车辆与车辆之间(vehicle to vehicle,V2V)的交互、车辆与人之间(vehicle to pedestrian,V2P)的交互、车辆与路侧单元之间(vehicle to infrastructure,V2I)的交互、车辆与网络之间(vehicle to network,V2N)的交互。另外,C-V2X包含了两种通信接口:一种是车辆、人、交通路侧基础设施之间的短距离直接通信接口(如,PC5,专用短程通信(dedicated short range communications,DSRC,即802.11P)),另一种是车辆和网络(如基站)之间的通信接口(如,Uu),可实现长距离和更大范围的可靠通信。

[0068] 本申请实施例主要是基于短距离直接通信接口(如,上述PC5或上述DSRC)的通信。也就是说,本申请实施例所述的发送设备101和接收设备102可以分别指车辆、人(行人设备)、交通路侧基础设施,两者可直接通过PC5进行V2X通信。在一些实施例中,发送设备101和接收设备102的设备形态可以相同,如发送设备101和接收设备102均为车辆。在另一些实施例中,发送设备101和接收设备102的设备形态也可以不同,如发送设备101为车辆,接收设备102为交通路侧基础设施。也就是说,本申请实施例可适用于车辆与车辆,车辆与行人设备,车辆与交通路侧基础设施,交通路侧基础设施与交通路侧基础设施等场景中。作为一种示例,图1中是以发送设备101和接收设备102均为车辆为例示出的。

[0069] 请参考图2,为本申请实施例提供的一种信息处理系统200的结构示意图。上述发送设备101和接收设备102中可设置该信息处理系统200,以用于实现V2X通信。如图2所示,该信息处理系统200可以包括:处理器210,存储器220,电源230,天线1,天线2,移动通信模块240,传感器模块250,定位模块260。信息处理系统200的各个器件之间可利用总线实现连接。

[0070] 可以理解的是,本实施例示意的结构并不构成对上述信息处理系统200的具体限定。在另一些实施例中,上述信息处理系统200可以包括比图示更多或更少的部件,或者组合某些部件,或者拆分某些部件,或者不同的部件布置。图示的部件可以以硬件,软件或软件和硬件的组合实现。

[0071] 其中,处理器210是信息处理系统200的控制中心,可以是一个处理器,也可以是多个处理元件的统称。例如,处理器210是一个中央处理器(central processing unit,CPU),也可以是特定集成电路(application specific integrated circuit,ASIC),或者是被配置成实施本申请实施例的一个或多个集成电路,例如:一个或多个微处理器(digital signal processor,DSP),或,一个或者多个现场可编程门阵列(field programmable gate

array,FPGA)。

[0072] 其中,处理器210可以通过运行或执行存储在存储器220内的软件程序,以及调用存储在存储器220内的数据,执行信息处理系统200的各种功能。另外,在本实施例中,处理器210还可用于收集包含该信息处理系统200的设备(如发送设备101或接收设备102)的状态信息。以车辆包含该信息处理系统200为例,处理器210可用于收集车辆的车门状态,气囊状态等车身信息。

[0073] 在具体的实现中,作为一种实施例,处理器210可以包括一个或多个CPU,例如处理器210包括CPU0和CPU1。在具体实现中,作为一种实施例,信息处理系统200可以包括多个处理器。这些处理器中的每一个可以是一个单核处理器(single-CPU),也可以是一个多核处理器(multi-CPU)。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据(例如计算机程序指令)的处理核。

[0074] 存储器220可以是随机存取存储器(random access memory,RAM)(如,图2中所示的双倍数据速率(double data rate,DDR)),图2中所示的闪存(flash),只读存储器(Read-Only Memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(electrically erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者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。存储器220可以是独立存在,通过总线与处理器210相连接。存储器220也可以和处理器210集成在一起。

[0075] 其中,存储器220可用于存储执行本申请方案的软件程序,并由处理器210来控制执行。存储器220还可用于存储本申请实施例中所述的身份信息的摘要和MAC地址的摘要。

[0076] 电源230,可用于为信息处理系统200的各个部件,如处理器210、存储器220等供电。

[0077] 信息处理系统200的无线通信功能可以通过天线1,天线2,移动通信模块240,定位模块260以及调制解调处理器等实现。

[0078] 天线1和天线2用于发射和接收电磁波信号。信息处理系统200中的每个天线可用于覆盖单个或多个通信频带。不同的天线还可以复用,以提高天线的利用率。例如:可以将天线1复用为无线局域网的分集天线。在另外一些实施例中,天线可以和调谐开关结合使用。

[0079] 移动通信模块240可以提供应用在信息处理系统200上的包括2G/3G/4G/5G等无线通信的解决方案。移动通信模块240可以包括至少一个滤波器,开关,功率放大器,低噪声放大器(low noise amplifier,LNA)等。移动通信模块240可以由天线1接收电磁波,并对接收的电磁波进行滤波,放大等处理,传送至调制解调处理器进行解调。移动通信模块240还可以对经调制解调处理器调制后的信号放大,经天线1转为电磁波辐射出去。在一些实施例中,移动通信模块240的至少部分功能模块可以被设置于处理器210中。在一些实施例中,移动通信模块240的至少部分功能模块可以与处理器210的至少部分模块被设置在同一个器件中。

[0080] 定位模块260可以提供全球导航卫星系统(global navigation satellite system,GNSS)的解决方案,以实现包含该信息处理系统200的设备(如发送设备101或接收设备102)的定位功能。定位模块260可经由天线2接收电磁波,将电磁波信号调频以及滤波处理,将处理后的信号发送到处理器210,以便处理器210确定设备的位置信息。

[0081] 在一些实施例中,信息处理系统200的天线1和移动通信模块240耦合,天线2和定位模块260耦合。另外,上述GNSS可以包括全球卫星定位系统(global positioning system,GPS),全球导航卫星系统(global navigation satellite system,GLONASS),北斗卫星导航系统(beidou navigation satellite system,BDS),准天顶卫星系统(quasi-zenith satellite system,QZSS)和/或星基增强系统(satellite based augmentation systems,SBAS)。

[0082] 传感器模块250,可以包括加速度传感器,角速度传感器等。

[0083] 其中,在一些实施例中,如果上述信息处理系统200被设置在车辆中,则信息处理系统200可以称为车载通信盒(telematics box,T-BOX),或称为车载通信控制单元(telematics Control Unit,TCU)。T-BOX或TCU是一种安装在车辆内部的可收集车身网络中其他电子控制单元(electronic control unit,ECU)状态信息的盒状ECU单元,如可收集车门状态,气囊状态等等信息,还可向车机提供3GPP/LTE的电信/移动/联通数据上网服务数据通道拨打ECALL呼叫。

[0084] 以下实施例中的方法均可以在具有上述硬件结构的设备(如上述发送设备101和接收设备102)中实现。

[0085] 图3为本申请实施例提供的一种身份验证方法的流程示意图。如图3所示,该方法可以包括:

[0086] S301、发送设备生成V2X报文,该V2X报文中携带第一摘要和第二摘要。

[0087] S302、发送设备发送上述V2X报文。

[0088] 其中,上述第一摘要是发送设备的身份信息的摘要,上述第二摘要是发送设备的MAC地址的摘要。发送设备在需要进行V2X通信时,可以计算出自身身份信息的摘要和MAC地址的摘要,即获得第一摘要和第二摘要,然后生成V2X报文。发送设备可广播携带第一摘要和第二摘要的V2X报文。另外,该V2X报文中还可以包括发送设备需要发送的其他数据。

[0089] S303、接收设备接收发送设备发送的V2X报文。

[0090] S304、接收设备根据已识别身份的设备列表,以及第一摘要和第二摘要,确定发送设备是否是已被接收设备识别身份的设备。

[0091] 其中,上述已识别身份的设备列表中可包括:已被接收设备识别身份的设备的身份信息的摘要和MAC地址的摘要。该已识别身份的设备列表可存储在接收设备中,如存储在接收设备的存储器中。在接收到V2X报文后,接收设备可以确定已识别身份列表中是否包括V2X报文中的第一摘要和第二摘要,也就是说,接收设备可以确定V2X报文中的第一摘要和第二摘要,是否与已识别身份的设备列表中存储的某组身份信息的摘要和MAC地址的摘要相同(或者说一致)。如果已识别身份的设备列表中包括第一摘要和第二摘要,即第一摘要和已识别身份的设备列表中存储的身份信息的摘要相同,且第二摘要和已识别身份的设备列表中存储的MAC地址的摘要相同,则接收设备可以确定发送设备是已被接收设备识别身份的设备。如果已识别身份的设备列表中未包括第一摘要和/或第二摘要,即:第一摘要和

已识别身份的设备列表中存储的身份信息的摘要相同，而第二摘要和已识别身份的设备列表中存储的MAC地址的摘要不同，或，第二摘要和已识别身份的设备列表中存储的MAC地址的摘要相同，而第一摘要和已识别身份的设备列表中存储的身份信息的摘要不同，或第一摘要和已识别身份的设备列表中存储的身份信息的摘要不同，且第二摘要和已识别身份的设备列表中存储的MAC地址的摘要不同，则接收设备可以确定发送设备未被接收设备识别身份。

[0092] 在接收设备确定出发送设备是已被接收设备识别身份的设备时，接收设备可以认为此次接收到的V2X报文中的数据是可信任的数据，因此可以利用V2X报文中的数据做相关处理。

[0093] 本申请实施例提供的身份验证方法，通过将V2X报文中目前规定需携带的身份信息隐式化，也就是说，采用由身份信息确定的摘要和由MAC地址确定的摘要替代，不以明文形式传送，即对外不直接暴露。这样，可提高身份信息传输的安全性。同时，对于接收方来说，通过对比存储的隐式数据来快速确认发送方的身份是否可信任。这样，大大减轻了消息验证负担，缩短了处理时延。

[0094] 为了便于本领域技术人员理解，以下实施例中结合图4-图6，以发送设备和接收设备均为车辆，如发送设备为车辆A，接收设备为车辆B，发送设备和接收设备之间通过V2X通信来交互车辆数据为例，对本申请实施例提供的一种身份验证方法进行详细说明。

[0095] 图4为本申请实施例提供的另一种身份验证方法的流程示意图。如图4所示，该方法可以包括：

[0096] S401、车辆A广播V2X报文，V2X报文中携带第一摘要和第二摘要。

[0097] 其中，第一摘要可以是车辆A的身份信息的摘要，第二摘要可以是车辆A的MAC地址的摘要。

[0098] 车辆A与车辆B在道路上行驶，且车辆A和车辆B均具备V2X通信的能力。车辆(如车辆A)可生成V2X报文，并广播V2X报文给道路上的其他车辆(如车辆B)以通知其相关信息。例如，V2X报文中可携带车辆A的车辆数据。

[0099] 在一些实施例中，车辆数据是指车辆与其他设备(如车辆，人，交通路侧基础设施等)之间交互的数据。例如，如表1所示，目前规范中定义的车辆数据可以包括：车辆身份信息，车辆尺寸信息，车辆位置信息，车辆速度，车辆方向盘转角信息等数据。

[0100] 表1

[0101]

车辆数据					
车辆身份信息	车辆尺寸信息	车辆位置信息	车辆速度	车辆方向盘转角信息	……

[0102] 其中，车辆身份信息可以是车辆识别号码(vehicle identification number，VIN)。VIN是一组由十七个英文或数字组成，用于标识车辆的一组独一无二的号码。通过这组号码，可以识别出车辆的生成商，引擎，底盘序号，以及其他性能资料。这个号码也与车辆行驶证上的车辆所有者的身份证号相关联，通过公路交通查询系统可获知车辆所有人的身份信息。可以理解，车辆身份信息属于敏感数据，如果按照目前规范中的定义采用明文传输，则会存在安全隐患。因此，本申请实施例中，对于V2X报文中需携带的身份信息，如车辆

身份信息采用密文代替明文，以来确保车辆身份信息在V2X通信过程中的安全性。另外，国标文档《合作式智能运输系统车用通信系统应用层及应用数据交互标准》(CSAE 53-2017)中定义，可采用BSM报文来实现车辆与其他设备之间车辆数据的交互，从而实现路面上车辆间的相互感知。因此，车辆A周期性广播的V2X报文具体的可以是BSM报文。

[0103] 示例性的，以V2X报文为BSM报文为例。如图5所示，车辆A在道路上行驶的过程中，可以判断是否需要发送BSM报文(即执行S501)，以使得周围的车辆(如车辆B)可以获得相关信息。

[0104] 如果需要发送BSM报文，为了保证V2X通信过程中车辆身份信息传输的安全性，车辆A可以执行S502，即生成BSM报文。其中，S502具体的可以是：车辆A利用消息摘要算法确定车辆A的车辆身份信息(如VIN)的摘要，以获得第一摘要。如第一摘要可以称为VIN摘要。车辆A利用消息摘要算法确定车辆A的MAC地址的摘要，以获得第二摘要。如第二摘要可以称为MAC地址摘要。车辆A还可获取车辆A的车辆尺寸信息，车辆位置信息，车辆速度，车辆方向盘转角信息等数据。在获得VIN摘要，MAC地址摘要以及上述数据后，车辆A可生成BSM报文。如表2所示，在该BSM报文中携带上述第一摘要(即VIN摘要)和第二摘要(MAC地址摘要)，以及车辆尺寸信息，车辆位置信息，车辆速度，车辆方向盘转角信息等车辆数据。在车辆A组织好BSM报文后，便可广播该BSM报文(即执行S503)。

[0105] 表2

[0106]

车辆数据					
VIN 摘要，MAC 地址摘要	车辆尺寸信息	车辆位置信息	车辆速度	车辆方向盘转角信息	……

[0107] 其中，可以理解的是，车辆尺寸信息，车辆位置信息，车辆速度，车辆方向盘转角信息等数据相较于车辆身份信息来说，敏感度低一些，因此可以采用明文传输。另外，对比表1和表2可知，在本申请实施例中，将目前规范定义的车辆身份信息替换为VIN摘要和MAC地址摘要。如，可将VIN摘要和MAC地址摘要串接后替代目前规范定义的车辆身份信息。本实施例中，对于VIN摘要和MAC地址摘要的串接前后顺序并不做具体限制。

[0108] 需要说明的是，对于路面上行驶的车辆，可以周期性的广播V2X报文给道路上的其他车辆，以便其他车辆能够获得更多的信息来进行相关处理。也就是说，车辆A可以周期性的执行上述S501-S503。在一些实施例中，由于车辆数据中的车辆位置信息，车辆速度，车辆方向盘转角信息等车辆数据可能是实时变化的，因此，在需要发送BSM报文时，需重新获取这些数据。而对于VIN摘要，MAC地址摘要等数据可能并不会变化，因此，车辆A可以在第一次获取到这些不变的数据后，将其存储，在后续生成BSM报文时可直接用存储的这些数据，而无需重新计算摘要。也就是说，在执行上述S502时，只有在第一次组织BSM报文时需计算出VIN摘要和MAC地址摘要(第一次计算出VIN摘要和MAC地址摘要后可将其存储)，后续无需计算可直接用存储的VIN摘要和MAC地址摘要来组织BSM报文。

[0109] S402、车辆B接收车辆A发送的上述V2X报文。

[0110] 其中，在车辆A广播V2X报文后，道路上车辆A附近的车辆，如车辆B将接收到车辆A广播的V2X报文。

[0111] 示例性的，以V2X报文为BSM报文为例。结合上述S401和图5中的示例，如图6所示，道路上行驶的车辆，如车辆B可监测是否接收到BSM报文(即执行S601)。如果监测结果是未

接收到，则可以重新执行S601。如果道路上的其他车辆，如车辆A广播了BSM报文，则车辆B将接收到车辆A广播的BSM报文。

[0112] S403、车辆B利用消息摘要算法确定接收到的V2X报文中携带的MAC地址的摘要，确定第二摘要与确定出的摘要相同。

[0113] 其中，在车辆A广播V2X报文时，该V2X报文中除了包含数据部分，如上述车辆数据外，还包含网络报文头。该网络报文头中携带有车辆A的MAC地址。在本申请实施例中，车辆B在接收到车辆A的V2X报文后，可以利用消息摘要算法确定出V2X报文的网络报文头中携带的MAC地址的摘要，然后判断该确定出的摘要与V2X报文中携带的第二摘要是否相同，从而确定该V2X报文是否是合法报文。如果确定出的摘要与第二摘要相同，则可以确定接收到的V2X报文是合法报文，此时可执行S404。如果确定出摘要与第二摘要不同，则可以确定接收到的V2X是非法报文，或者说是无效报文，此时可将接收到的报文丢弃。

[0114] 示例性的，以V2X报文为BSM报文为例。结合上述S401-S402，以及图5和图6中的示例。如图6所示，如果车辆B接收到车辆A广播的BSM报文，车辆B可以利用消息摘要算法确定该BSM报文的网络报文头中携带的MAC地址的摘要，并判断确定出的MAC地址的摘要与BSM报文中携带的MAC地址摘要是否一致(即执行S602)。如果确定出的MAC地址的摘要与BSM报文中携带的MAC地址摘要是不一致，则可确定接收到的BSM报文为无效报文，可将该报文丢弃(即执行S603)。在将接收到的报文丢弃后，车辆B还可重新执行上述S601，以便及时获取其他的BSM报文。如果确定出的MAC地址的摘要与BSM报文中携带的MAC地址摘要一致，则可执行以下S604。

[0115] S404、车辆B根据已识别身份的设备列表中包括的身份信息的摘要和MAC地址的摘要，以及第一摘要和第二摘要，确定车辆A是否是已被车辆B识别身份的设备。

[0116] 对于车辆B接收到的V2X报文，车辆B可以从V2X报文中获得其携带的数据，如第一摘要和第二摘要，当然还可有其他明文数据。由于消息摘要算法具有不可逆性，因此，车辆B无法根据用于指示身份信息的第一摘要和第二摘要确定出发送方的身份。这样，车辆B也无法确定接收到的V2X报文是否真实有效(或者说是否可信)。

[0117] 在本实施例中，为了能够降低处理时延和消息验证负担，车辆B中可以存储有已识别身份的设备列表，该已识别身份的设备列表中包括已被车辆B识别身份的设备的身份信息的摘要和MAC地址的摘要。这样，在接收到V2X报文时，车辆B便可根据存储的已识别身份的设备列表来确认发送方的身份，即确定车辆A是否是已被车辆B识别身份的设备。

[0118] 如果车辆B确定已识别身份的设备列表中包括第一摘要和第二摘要，即第一摘要和已识别身份的设备列表中存储的身份信息的摘要相同，且第二摘要和已识别身份的设备列表中存储的MAC地址的摘要相同，则可以确定车辆A是已被车辆B识别身份的设备，此时，车辆B可执行以下S405。如果车辆B确定已识别身份的设备列表中未包括第一摘要和/或第二摘要，即：第一摘要和已识别身份的设备列表中存储的身份信息的摘要相同，但第二摘要和已识别身份的设备列表中存储的MAC地址的摘要不同，或者车辆B确定第二摘要和已识别身份的设备列表中存储的MAC地址的摘要相同，但第一摘要和已识别身份的设备列表中存储的身份信息的摘要不同，或者车辆B确定第一摘要和已识别身份的设备列表中存储的身份信息的摘要不同，且第二摘要和已识别身份的设备列表中存储的MAC地址的摘要不同，则车辆B可以确定车辆A未被车辆B识别身份。在确定车辆A未被车辆B识别身份时，车辆B可执

行以下S406-S408,以确认车辆A的身份。

[0119] 示例性的,以V2X报文为BSM报文为例。结合上述S401-S403,以及图5和图6中的示例。车辆B接收到BSM报文后,车辆B可获得BSM报文中的相关数据,即VIN摘要,MAC地址摘要,以及其他明文数据,如车辆尺寸信息,车辆位置信息,车辆速度,车辆方向盘转角信息等。但车辆B无法确认VI N摘要和MAC地址摘要所指示的车辆身份。如图6所示,如果在上述S602中车辆B确定出的MAC地址的摘要与BSM报文中携带的MAC地址摘要是一致的,则车辆B可执行S604。S604具体的可以为:车辆B判断已识别身份的设备列表中存储的车辆身份信息的摘要和MAC地址的摘要,是否与BSM报文中携带的VIN摘要和MAC地址摘要一致(或者说,车辆B判断已识别身份的设备列表中是否包含VIN摘要和MAC地址)。

[0120] 如果车辆B确定VIN摘要和已识别身份的设备列表中存储的身份信息的摘要一致,且MAC地址摘要和已识别身份的设备列表中存储的MAC地址的摘要一致,即确定已识别身份的设备列表中包含VIN摘要和MAC地址,则可以确定车辆A是已被车辆B识别身份的设备,此时,车辆B可认为接收到的BSM报文中的数据是可信的,车辆B可执行S605。即车辆B可以利用BSM报文中的车辆数据进行相关处理。

[0121] 如果车辆B确定VIN摘要和已识别身份的设备列表中存储的身份信息的摘要一致,但MAC地址摘要和已识别身份的设备列表中存储的MAC地址的摘要不一致,或者车辆B确定MAC地址摘要和已识别身份的设备列表中存储的MAC地址的摘要一致,但VIN摘要和已识别身份的设备列表中存储的身份信息的摘要不一致,或者车辆B确定VI N摘要和已识别身份的设备列表中存储的身份信息的摘要不一致,且MAC地址摘要和已识别身份的设备列表中存储的MAC地址的摘要不一致,即确定已识别身份的设备列表中不包含VIN摘要和/或MAC地址,则车辆B可以确定车辆A未被车辆B识别身份,此时,车辆B可执行以下S606-S607,以确认车辆A的身份。

[0122] S405、车辆B利用V2X报文中的数据进行相关处理。

[0123] 例如,车辆B在确认接收到的BSM报文的数据可信后,车辆B如果采用自动驾驶模式,则可以依据BSM报文中的数据(如,车辆位置信息,车辆速率等)判断本车的速度,位置是否需要调整,如是否需要进行避让。又例如,车辆B在确认接收到的BSM报文的数据可信后也可以将BSM报文中的数据收集起来,进而作为当前行驶路段是否拥堵的判断依据。

[0124] S406、车辆B获取车辆A的身份信息和车辆A的MAC地址。

[0125] 其中,车辆B可以通过发送身份请请求报文,以获得车辆A的身份信息和车辆A的MAC地址。具体的,车辆B可以广播身份请求报文。该身份请求报文中可携带接收到的V2X报文中的第一摘要和第二摘要。这样,道路上处于车辆B附近的车辆,如车辆A将接收到该身份请求报文。车辆A接收到该身份请求报文后,可判断该身份请求报文中携带的第一摘要和第二摘要是否与自身的身份信息的摘要和MAC地址的摘要一致。如果第一摘要与自身的身份信息的摘要一致,且第二摘要与自身的MAC地址的摘要一致,则车辆A可以对该身份请求报文进行响应。为了不泄露隐私,车辆A可以以全密文的形式将自身的身份信息和MAC地址广播出去。也就是说,车辆A可广播身份响应报文,该身份响应报文中携带加密的车辆A的身份信息和加密的车辆A的MAC地址。这样,道路上处于车辆A附近的车辆,如车辆B将接收到该身份响应报文。车辆B接收到该身份响应报文后,可分别对加密的车辆A的身份信息和加密的车辆A的MAC地址进行解密,以获得车辆A的身份信息明文和车辆A的MAC地址明文。

[0126] 示例性的，以V2X报文为BSM报文为例。结合上述S401-S404，以及图5和图6中的示例。如图6所示，在车辆B确定车辆A未被车辆B识别身份时，车辆B可启动V2X通信的交互流程，以DSA报文类型交互流程广播身份请求报文为例，即车辆B可执行S606：生成DSA请求报文(该专用短程通信业务公告(DSRC service advertisement，DSA)请求报文即为上述身份请求报文)和S607：车辆B广播该DSA请求报文。其中，该DSA请求报文中可携带接收到的BSM报文中携带的VIN摘要和MAC地址摘要。

[0127] 继续参见图5所示，处于车辆B周围的车辆A将接收到该DSA请求报文(即执行S504)。车辆A接收到该DSA请求报文后，可判断该DSA请求报文中携带的VIN摘要和MAC地址摘要是否与自身的车辆身份信息的摘要和MAC地址的摘要一致(即执行S505)。如果VIN摘要与自身的车辆身份信息的摘要不一致，和/或，MAC地址摘要与自身的MAC地址的摘要不一致，则车辆A可以丢弃该DSA请求报文。如果VIN摘要与自身的车辆身份信息的摘要一致，且MAC地址摘要与自身的MAC地址的摘要一致，则车辆A可以对该DSA请求报文进行响应，即执行S506：车辆A将自身的车辆身份信息与MAC地址进行加密后广播出去。其中，车辆A加密车辆身份信息和MAC地址的方法可以为：车辆A采用对称加密算法(如高级加密标准(advanced encryption standard，AES算法))将车辆A的车辆身份信息与MAC地址加密成密文数据。如车辆A的车辆身份信息与MAC地址的加密密钥为密钥A。然后，车辆A将密钥A使用非对称加密算法(如RSA算法)加密后串接在密文数据后得到DSA响应报文(DSA响应报文即为上述身份响应报文)。其中密钥A的加密秘钥可以使用车辆A的私钥。最后将该DSA响应报文广播出去。可选的，车辆A在接收到DSA请求报文后，可以先判断该DSA请求报文是否是请求身份的报文，如果是请求身份的报文，则执行上述S505。如果不是请求身份的报文，则可按照DSA请求报文中的内容做相应处理。这样可实现与现有DSA请求报文的兼容。

[0128] 继续参见图6所示，道路上处于车辆A附近的车辆B将接收到该DSA响应报文。车辆B接收到该DSA响应报文后，可执行S608：获取车辆A的车辆身份信息明文和车辆A的MAC地址明文。具体的，车辆B可根据车辆B的公钥对DSA响应报文中加密的密钥A进行解密，以获得加密数据的加密秘钥，即获得密钥A。然后，车辆B采用该密钥A对DSA响应报文中的密文数据行解密，便可获得车辆A的车辆身份信息明文和MAC地址明文。

[0129] S407、车辆B利用消息摘要算法分别确定车辆A的身份信息的摘要和车辆A的MAC地址的摘要。

[0130] S408、在确定第一摘要与确定出的车辆A的身份信息的摘要相同，且第二摘要与确定出的车辆A的MAC地址的摘要相同时，车辆B将第一摘要和所述第二摘要存储在已识别身份的设备列表中。

[0131] 在车辆B获取到车辆A的身份信息明文和MAC地址明文后，车辆B可利用消息摘要算法对车辆A的身份信息进行运算，以得到车辆A的身份信息的摘要，利用消息摘要算法对车辆A的MAC地址进行运算，以得到车辆A的MAC地址的摘要。然后，车辆B可将计算出的摘要，与S402中接收到的V2X报文中的第一摘要和第二摘要进行对比。如果第一摘要与确定出的车辆A的身份信息的摘要相同，且第二摘要与确定出的车辆A的MAC地址的摘要相同，则车辆B核实了车辆A的身份。此时，车辆B可将该第一摘要和第二摘要存储在已识别身份的设备列表中。这样，如果后续继续接收到车辆A的V2X报文，则可直接通过对比接收到V2X报文中携带的摘要是否与已识别身份的设备列表中存储的摘要(包括身份信息的摘要和MAC地址的

摘要)是否一致,来确定发送V2X报文的车辆是否是已被车辆B识别身份的设备。另外,在核实了车辆A的身份后,车辆B还可利用接收到的V2X报文中的数据进行相关处理。

[0132] 示例性的,继续参见图6所示,在车辆B获取到车辆A的车辆身份信息明文和MAC地址明文后,车辆B可执行S609:车辆B将车辆A的车辆身份信息的摘要和车辆A的MAC地址的摘要,与接收到的BSM报文中的VIN摘要和MAC地址摘要进行对比。如果VIN摘要与车辆A的车辆身份信息的摘要相同,且MAC地址摘要与车辆A的MAC地址的摘要相同,则核实了车辆A的身份。车辆B可将该VIN摘要和MAC地址摘要存储在已识别身份的设备列表中。车辆B还可利用接收到的BSM报文中的数据进行相关处理。

[0133] 可选的,在获取到车辆A的身份信息和车辆A的MAC地址之后,S407之前,车辆B还可以先判断接收到的V2X报文的网络报文头中的MAC地址,与S406中获取到的MAC地址是否一致。如果两者一致,则认为S402中接收到的V2X报文是合法的报文,可执行S407-S408。如果两者不一致,则认为S402中接收到的V2X报文是不合法的报文,可将该报文丢弃。

[0134] 在本申请实施例中,为了进一步的提高信息的安全性,车辆B可在已识别身份的设备列表中包括的某对身份信息的摘要和MAC地址的摘要保存超过第一时长,如一个随机时间后(随机时间可分布在最小值和最大值之间),将该身份信息的摘要和MAC地址的摘要从已识别身份的设备列表中删除。如,参见图6中的S610:车辆B可从已识别身份的设备列表中删除对应的VIN摘要和MAC地址摘要。在删除了对应信息后,如车辆B再一次接收到了来自车辆A的V2X报文(如BSM报文)时,车辆B可重新执行上述S406-S408来确认发送方的身份。

[0135] 另外,按照《交通运输数字证书格式》,和《基于LTE的车联网通信安全总体技术要求》所定义的规范在V2X报文(如BSM报文)中,可在数据部分后名追加对该数据部分的签名数据(加密的)和证书数据(加密的)。也就是说,上述S401中的V2X报文除了包含网络报文头和数据部分(如包括第一摘要和第二摘要的车辆数据)外,还可包括签名数据和证书数据。这样,在车辆B接收到V2X报文后,可根据规范的要求对接收到的报文进行证书验证和签名验证,以用于确保接收到的报文的完整性和可靠性。在本申请实施例中,可以在验证完车辆的身份,即确认车辆A是否是车辆B已识别身份的设备后,再进行证书验证和签名验证。也可以先进行证书验证和签名验证,即在证书验证和签名验证均通过后,在验证车辆身份。本申请实施例对此不做限制。

[0136] 类似的,上述DSA响应报文也可以包含签名数据和证书数据。也就是说,车辆A在对数据加密,对加密密钥加密后,再追加签名数据和证书数据,得到DSA响应报文,并广播该DSA响应报文。相应的,车辆B接收到DSA响应报文后,也需先根据规范的定义接收到的DSA响应报文进行证书验证和签名验证,确认其完整性和可靠性。在完成确认后,再对从报DSA响应文中获取车辆A的车辆身份信息明文和MAC地址明文。需要说明的是,对于车辆追加签名数据和证书数据,以及进行证书验证和签名验证的具体过程,可参考《交通运输数字证书格式》,和《基于LTE的车联网通信安全总体技术要求》中的定义,本申请实施例在此不予赘述。

[0137] 可以理解的是,上述实施例中是以在进行V2X通信时,将设备的身份信息,如车辆的车辆身份信息用密文(即身份信息的摘要和MAC地址的摘要)替代来确保身份信息的安全性为例进行说明的。当然,除了身份信息外,有些数据也是比较敏感的。例如,在车辆数据中车辆尺寸信息、车辆类型等也是比较敏感的数据,本申请实施例将这些敏感数据称为隐私信息。在本申请实施例中,也可以对这些隐私信息用密文代替明文,以确保其传输的安全

性。

[0138] 示例性的，以隐私信息为设备的尺寸信息，如车辆尺寸信息为例，可以将车辆尺寸信息进行加密传输。如，上述S401中的V2X报文中除了包含第一摘要和第二摘要外，还可携带第三摘要。该第三摘要是车辆A的车辆尺寸信息的摘要。车辆A可以利用消息摘要算法确定出车辆A的车辆尺寸信息的摘要，以获得该第三摘要，并用其替代目前规范定义的车辆尺寸信息明文。车辆B接收到包含第一摘要，第二摘要和第三摘要的V2X报文后，可以在利用第一摘要和第二摘要确定出车辆A是已被车辆B识别身份的设备后，根据已识别身份的设备列表中存储的尺寸信息的摘要和第三摘要，确定该第三摘要是否是可信任数据。其中，如果第三摘要和已识别身份的设备列表中存储的尺寸信息的摘要相同，则第三摘要是可信任数据；如果第三摘要和已识别身份的设备列表中存储的尺寸信息的摘要不同，则第三摘要是不可信任数据。在确定出第三摘要是可信任数据后，车辆B可利用该第三摘要，即车辆尺寸信息的摘要进行相关处理。当然，如果车辆B确定第三摘要是不可信任数据，则可以获取车辆A的车辆尺寸信息，并利用消息摘要算法确定车辆A的车辆尺寸信息的摘要，并在确定V2X报文中的第三摘要与确定出的车辆A的尺寸信息的摘要相同时，将该第三摘要存储在已识别身份的设备列表中。还可确定该第三摘要是可信任数据，利用其进行相关处理。其中，车辆B获取车辆A的车辆尺寸信息的过程可以参考上述S406中的描述，也就是说，在车辆B执行S406的过程中，也可以获得该车辆A的车辆尺寸信息明文。

[0139] 另外，在本实施例中，除了设备的身份信息外，其他的数据，即上述隐私信息是否加密可以是可选的。其中，可以通过在对某数据加密时，采用一加密标志来告知接收方该数据是加密的，而在该数据未加密时，采用一未加密标志来告知接收方该数据未加密。例如，结合上述示例，如果车辆A对车辆尺寸信息采用密文传输，则可以在车辆尺寸信息的摘要，如上述第三摘要前添加加密标志来告知接收方该车辆尺寸信息是加密的。如果车辆A对车辆尺寸信息采用明文传输，则可以在车辆尺寸信息明文前添加未加密标志来告知接收方该车辆尺寸信息是明文。

[0140] 需要说明的是，在本申请实施例中，所述的消息摘要算法可以是HASH算法或SM3算法等。另外，接收设备和发送设备需采用相同的消息摘要算法进行摘要运算。其中，HASH，一般翻译做“散列”，也可直接音译为“哈希”。其是把任意长度的输入(又叫做预映射pre-image)通过HASH算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间。不同的输入可能会散列成相同的散列值，所以不可能从散列值来确定唯一的输入值，也即其是不可逆的。简单的说，HASH算法是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。SM3与NASH类似。可以理解是，由于不同的输入进行HASH求得的摘要结果有一定几率完全一致(称为碰撞)，根据相关分析，找到安全散列算法(secure hash algorithm，SHA)-256的一个碰撞，其复杂度为2^66，也就是有2^66分之一的几率可能会产生碰撞。本申请中由于采用了身份信息的摘要加MAC地址的摘要来替代身份信息明文，使得碰撞的几率更低，为2^132分之一几率，大大降低了碰撞可能。

[0141] 上述技术方案，通过将V2X报文中目前规定需携带的身份信息隐式化，也就是说，采用由身份信息确定的摘要和由MAC地址确定的摘要替代，不以明文形式传送，从而达到车辆A与车辆B在进行V2V通信过程中，全程没有暴露车辆的身份信息。提高了身份信息传输的

安全性。另外，V2X报文中的其他数据也会变成主体身份无法识别的无价值数据，降低了V2X报文中的其他数据，如车辆数据被利用的价值和可能。同时，对于接收方来说，仅在第一次接收到包含该隐式化敏感数据的V2X报文后需要通过验证过程来验证确认发送方的身份，后续不再对发送方的数据进行复杂的验证，而是通过对比存储的隐式数据来确认发送方的身份。这样，大大减轻了消息验证负担，缩短了处理时延。另外，采用本申请的方案无需增加任何器件成本，也无需做复杂的软件设计，具备良好的可用性，可实现性和成本效益。本申请的方案可使V2X通信的安全性环境更加健壮，利于未来智能车联网应用的快速部署。

[0142] 另外，本申请的方案没有显著增加发送方和接收方的密码学操作负担，且对原有报文的格式修改非常小，使得软件几乎可以立即完成修改和实现，并且不影响原有报文传输形式，在启动成本和周期上具有明显优势。本申请方案也未增加任何私有密码学算法，使用通用的HASH算法即可实现，具备良好的可实现性。本申请方案也不会导致区域网络中的报文数量激增，对LTE-V这类网络资源负载敏感的通信协议来说具备更好的可部署性和可承载性。本申请的方案对发送方来说是一种可双向选择的自适应协议，发送方可自行根据自身情况发起或者不发起身份验签流程。其不会因为本申请所述的方法而导致原有软硬件处理流程受到影响，也不会对原有软件处理流程构成扰乱，具备良好的向前兼容性。

[0143] 可以理解的，在上述车辆A与车辆B进行V2X通信的过程中，如果存在恶意车辆，那么恶意车辆也可以接收到车辆A发送的V2X报文。但是由于V2X报文中是采用密文(身份信息的摘要和MAC地址的摘要)传输车辆A的身份信息的，因此恶意车辆并不能获知接收到的V2X报文是那个车辆发出的。当然，恶意车辆也会接收到车辆A发送的身份响应报文。但身份响应报文是全密文(需要基于CA证书的私钥进行解密)的，由于其无法通过CA机构获得授权，无法得到私钥，也就无法解密密文，从而不能获得车辆A的身份信息明文和MAC地址明文。

[0144] 如果恶意车辆直接利用车辆A的V2X报文中的身份信息的摘要和MAC地址的摘要，冒充车辆A广播V2X报文。车辆B接收到该冒充的V2X报文后，可以核对出其V2X报文的网络报文头中的MAC地址的摘要和V2X报文中的携带的MAC地址的摘要是不一致的，此时可确定其是非法报文，可将其丢弃。又例如，恶意车辆利用车辆A的V2X报文中的身份信息的摘要和自身的MAC地址的摘要冒充车辆A广播V2X报文。车辆B在接收到该冒充的V2X报文后，虽然可核对出其V2X报文的网络报文头中的MAC地址的摘要和V2X报文中的携带的MAC地址的摘要一致的，但是，会确定出其报文中携带的身份信息的摘要与已识别身份的设备列表中存储的身份信息一致，但报文中携带的MAC地址的摘要与已识别身份的设备列表中存储的MAC地址摘要不一致，此时车辆B还可确定出接收到的V2X报文是非法报文，可将其丢弃。

[0145] 以下介绍一些应用实例：

[0146] 例如，小王是个不法人士，自己通过非正规渠道组装了一台具备LTE-V2X数据接收功能的设备终端装在车上或者其他装置上，打算用该设备的LTE-V2X通信能力专门收集路面其他车辆发送出来的BSM报文中相关车辆数据如车辆身份信息，车辆位置信息等。由于车辆身份信息可以识别到车辆身份，车辆身份又与驾驶者身份挂钩，小王想通过大规模记录相关数据去网上兜售以获利。而在车辆使用了本申请方案，即在发送BSM报文时使用自车的车辆身份信息的摘要和MAC地址的摘要时，由于消息摘要算法的不可逆性，无法通过摘要推导出原始信息，使得小王无法有效确认这些车辆的身份明文到底是什么，最终使得小王无法得逞。且这些车辆的其他车辆数据也会变成主体身份无法识别的无价值数据。

[0147] 又例如，小李设计了一个可以基于V2X通信实现车辆和车辆间直接或间接互动的应用，周边车辆可以相互之间直接点评，如点赞，扔番茄等等。由于涉及隐私追踪问题，小李希望被点赞或者仍番茄的车辆无法确定主动进行该动作的车辆，小李使用了本申请的方法，如某一时刻车C想告知车A，周边的车B有不文明驾驶等信息，车C在BSM报文中广播的是自车的车辆身份信息的摘要和MAC地址的摘要，无法推导出身份信息明文，所以车C并没有暴露身份信息，导致其他车辆都无法直接知晓该知会车辆的身份，使得该应用场景可以安全实现。

[0148] 再例如，小A是一个危险黑客，某一天他守在某一路口想通过他所设计的装置和软件来追踪小B，他将小B所驾驶车辆的品牌，型号都提前录入好，一旦程序制动识别到小B车辆的车辆身份信息后就会自动通知小A。但是小B使用了本申请所述提供的方案，其的车辆不再发送车辆的身份信息明文，而是只发送车辆身份信息的摘要和MAC地址的摘要。这样，小B从路口驶过时，小A的装置与软件没有触发通知，小A的监控失败。

[0149] 可以看到的是，车辆的身份信息不会泄露，且恶意车辆的仿冒和欺诈行为也无法成功的。

[0150] 本申请实施例可以根据上述方法示例对上述接收设备以及发送设备进行功能模块的划分，例如，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。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。

[0151] 请参考图7，其示出本申请实施例提供的一种接收设备的组成示意图。如图7所示，该接收设备可以包括：接收单元701、确定单元702、获取单元703以及存储单元704。

[0152] 接收单元701，用于接收发送设备发送的携带第一摘要和第二摘要的V2X报文。如上述方法实施例中的S303、S402。其中，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的MAC地址的摘要。确定单元702，用于根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备，如上述实施例中的S304、S404、S604；如果已识别身份的设备列表中未包括第一摘要和/或第二摘要，则确定发送设备未被接收设备识别身份。获取单元703，用于获取发送设备的身份信息和发送设备的MAC地址，如上述实施例中的S406。确定单元702，还用于利用消息摘要算法分别确定发送设备的身份信息的摘要和发送设备的MAC地址的摘要，如上述实施例中的S407。存储单元704，用于在确定单元确定第一摘要与确定出的发送设备的身份信息的摘要相同，且第二摘要与确定出的发送设备的MAC地址的摘要相同时，将第一摘要和第二摘要存储在已识别身份的设备列表中，如上述实施例中的S408。

[0153] 其中，确定单元702和获取单元703的功能可以集成在一个单元中，如称为综合逻辑处理单元。

[0154] 进一步的，确定单元702，还可以用于如果已识别身份的设备列表中包括第一摘要和第二摘要，则确定发送设备是已被接收设备识别身份的设备，并确定V2X报文中的数据是可信任数据。在确定单元702确定V2X报文中的数据是可信任数据时，接收设备便可利用V2X报文中的数据进行相关处理。

[0155] 进一步的，该接收设备还可以包括：发送单元705。

[0156] 发送单元705，可用于发送携带第一摘要和第二摘要的身份请求报文。接收单元701，还用于接收发送设备发送的身份响应报文，该身份响应报文中携带加密的发送设备的身份信息和加密的发送设备的MAC地址。获取单元703，具体用于分别对加密的发送设备的身份信息和加密的发送设备的MAC地址进行解密，获得发送设备的身份信息和发送设备的MAC地址。

[0157] 其中，接收单元701和发送单元705的功能可以集成在一个单元中，如称为信息收发单元。其可通过其连接的天线实现数据的收发。

[0158] 进一步的，确定单元702，还可用于确定获取到的发送设备的MAC地址与V2X报文中携带的MAC地址一致。

[0159] 进一步的，存储单元704，还可用于在第一时长后从已识别身份的设备列表中删除第一摘要和第二摘要。

[0160] 进一步的，确定单元702，还用于利用消息摘要算法确定V2X报文中携带的MAC地址的摘要；确定第二摘要与确定出的V2X报文中携带的MAC地址的摘要相同，如上述实施例中的S403、S602。

[0161] 进一步的，V2X报文中还可携带第三摘要，第三摘要是发送设备的隐私信息的摘要。确定单元702，具体用于在确定已识别身份的设备列表中包括第三摘要时，确定第三摘要是可信任数据。

[0162] 进一步的，获取单元703，还可用于如果确定单元702确定已识别身份的设备列表中未包括第三摘要，则获取发送设备的隐私信息。确定单元702，还用于利用消息摘要算法确定发送设备的隐私信息的摘要。存储单元704，还可用于在确定单元确定第三摘要与确定出的发送设备的隐私信息的摘要相同时，将第三摘要存储在已识别身份的设备列表中。

[0163] 当然，上述接收设备中的单元模块包括但不限于上述接收单元701、确定单元702、获取单元703、存储单元704以及发送单元705。例如，接收设备中还可以包括车辆数据采集单元，传感器数据采集单元，位置信息采集单元等。

[0164] 另外，当确定单元702和获取单元703的功能集成在一个单元中，如称为综合逻辑处理单元中时，该综合逻辑处理单元为一个或多个处理器(如图2所示的处理器210)，存储单元704可以为存储器(如图2所示的存储器220)，接收单元701和发送单元705的功能集成在一个单元中，如称为信息收发单元时，该信息收到单元可以为移动通信单元(如图2中所示的移动通信模块240)。本实施例所提供的接收设备可以为包括图2所示的信息处理系统的接收设备。其中，上述一个或多个处理器、存储器和移动通信模块等可以连接在一起，例如通过总线连接。存储器用于保存计算机程序代码，计算机程序代码包括指令。当处理器执行该指令时，电子设备可执行上述实施例中的相关方法步骤实现上述实施例中的方法。

[0165] 请参考图8，其示出本申请实施例提供的一种发送设备的组成示意图。如图8所示，该发送设备可以包括：生成单元801、接收单元802以及发送单元803。

[0166] 生成单元801，用于生成携带第一摘要和第二摘要的V2X报文，如上述实施例中的S301、S502。其中，第一摘要是发送设备的身份信息的摘要，第二摘要是发送设备的媒体访问控制MAC地址的摘要。发送单元803，用于发送V2X报文，如上述实施例中的S302、S401、S503。接收单元802，用于接收携带第一摘要和第二摘要的身份请求报文.如上述实施例中的S504。发送单元803，还用于发送身份响应报文，该身份响应报文中携带加密的发送设备

的身份信息和加密的发送设备的MAC地址，如上述实施例中的S506。

[0167] 进一步的，生成单元801，具体用于利用消息摘要算法确定发送设备的身份信息的摘要，以获得第一摘要；利用消息摘要算法确定发送设备的MAC地址的摘要，以获得第二摘要；生成V2X报文，V2X报文中携带第一摘要和第二摘要。

[0168] 进一步的，V2X报文中还可携带第三摘要；生成单元801，还用于利用消息摘要算法确定发送设备的隐私信息的摘要，以获得第三摘要。

[0169] 当然，上述发送设备中的单元模块包括但不限于上述生成单元801、接收单元802以及发送单元803。例如，发送设备中还可以包括存储单元，车辆数据采集单元，传感器数据采集单元，位置信息采集单元等。且接收单元802和发送单元803的功能可以集成在一个单元中，如称为信息收发单元。其可通过其连接的天线实现数据的收发。另外，上述生成单元也可称为综合逻辑处理单元，该综合逻辑处理单元为一个或多个处理器(如图2所示的处理器210)，接收单元802和发送单元803的功能集成在一个单元中，如称为信息收发单元时，该信息收到单元可以为移动通信单元(如图2中所示的移动通信模块240)。本实施例所提供的发送设备可以为包括图2所示的信息处理系统的发送设备。其中，上述一个或多个处理器、存储器和移动通信模块等可以连接在一起，例如通过总线连接。存储器用于保存计算机程序代码，计算机程序代码包括指令。当处理器执行该指令时，电子设备可执行上述实施例中的相关方法步骤实现上述实施例中的方法。

[0170] 本申请实施例还提供一种计算机可读存储介质，该计算机存储介质中存储有计算机软件指令，当计算机软件指令在信息处理装置中运行时，信息处理装置可执行上述实施例中的相关方法步骤实现上述实施例中的方法。

[0171] 本申请实施例还提供了一种计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行上述实施例中的相关方法步骤实现上述实施例中的方法。

[0172] 其中，本申请实施例提供的信息处理装置，发送设备，接收设备，计算机存储介质或者计算机程序产品均用于执行上文所提供的对应的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

[0173] 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。

[0174] 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。

[0175] 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。

[0176] 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。

[0177] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个可读取存储介质中。基于这样的理解，本申请实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该软件产品存储在一个存储介质中，包括若干指令用以使得一个设备(可以是单片机，芯片等)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0178] 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。


101
102
设备间进行V2X通信

图1

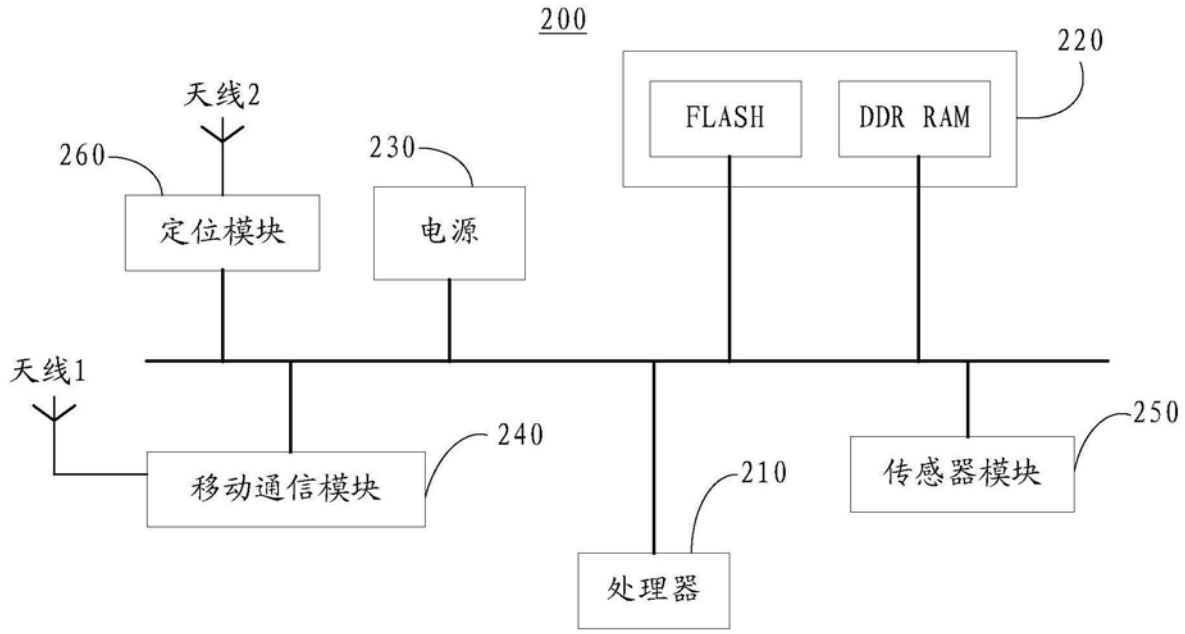

200
220
FLASH
DDR RAM
天线2
260
定位模块
230
电源
天线1
移动通信模块
240
210
处理器
传感器模块
250

图2

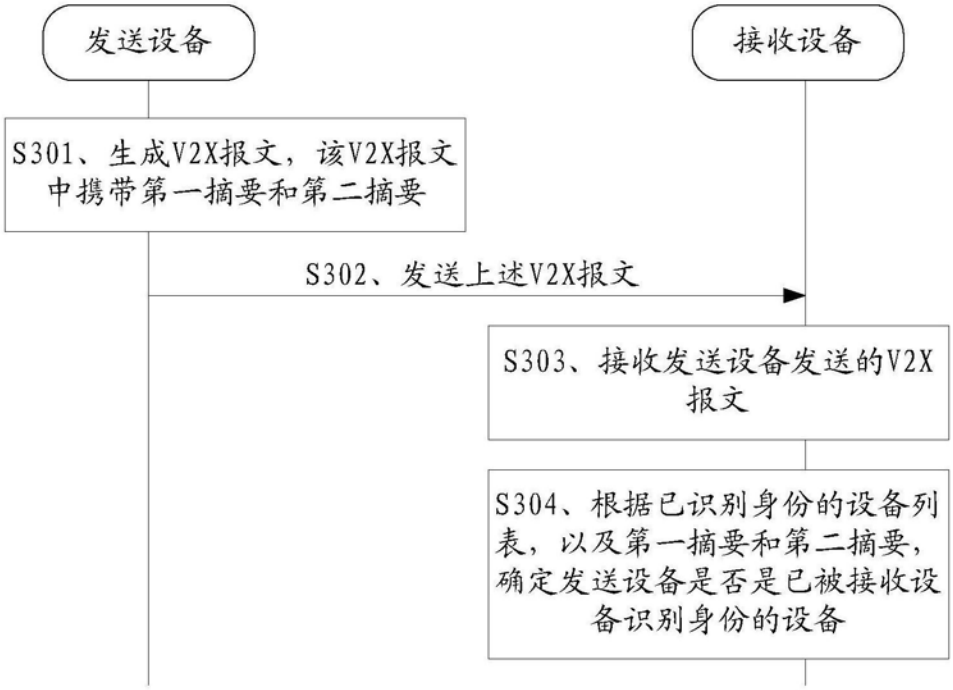

发送设备
接收设备
S301、生成V2X报文，该V2X报文中携带第一摘要和第二摘要
S302、发送上述V2X报文
S303、接收发送设备发送的V2X报文
S304、根据已识别身份的设备列表，以及第一摘要和第二摘要，确定发送设备是否是已被接收设备识别身份的设备

图3

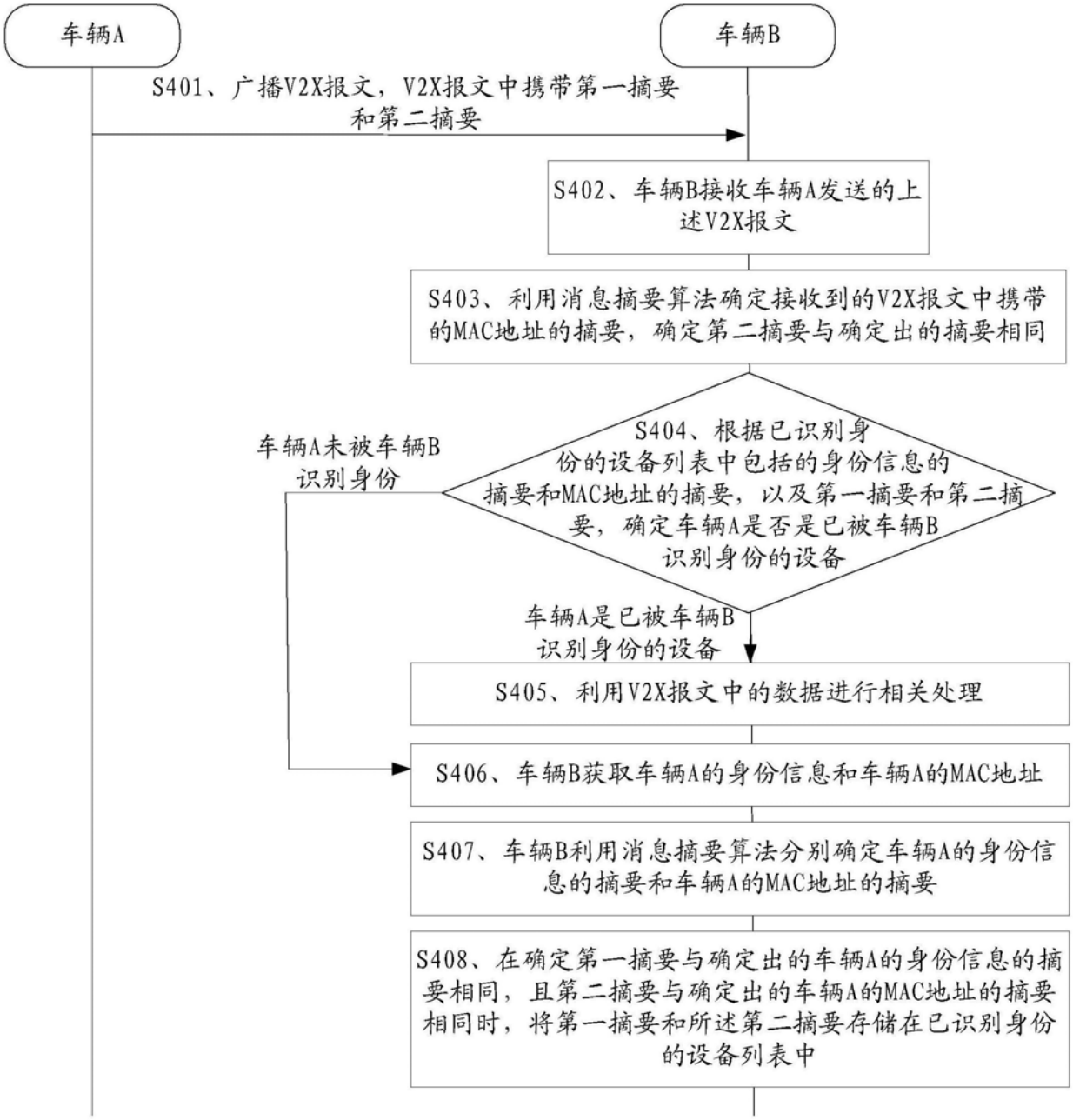

车辆A
车辆B
S401、广播V2X报文，V2X报文中携带第一摘要和第二摘要
S402、车辆B接收车辆A发送的上述V2X报文
S403、利用消息摘要算法确定接收到的V2X报文中携带的MAC地址的摘要，确定第二摘要与确定出的摘要相同
S404、根据已识别身份的设备列表中包括的身份信息的摘要和MAC地址的摘要，以及第一摘要和第二摘要，确定车辆A是否是已被车辆B识别身份的设备
车辆A未被车辆B识别身份
车辆A是已被车辆B识别身份的设备
S405、利用V2X报文中的数据进行相关处理
S406、车辆B获取车辆A的身份信息和车辆A的MAC地址
S407、车辆B利用消息摘要算法分别确定车辆A的身份信息的摘要和车辆A的MAC地址的摘要
S408、在确定第一摘要与确定出的车辆A的身份信息的摘要相同，且第二摘要与确定出的车辆A的MAC地址的摘要相同时，将第一摘要和所述第二摘要存储在已识别身份的设备列表中

图4

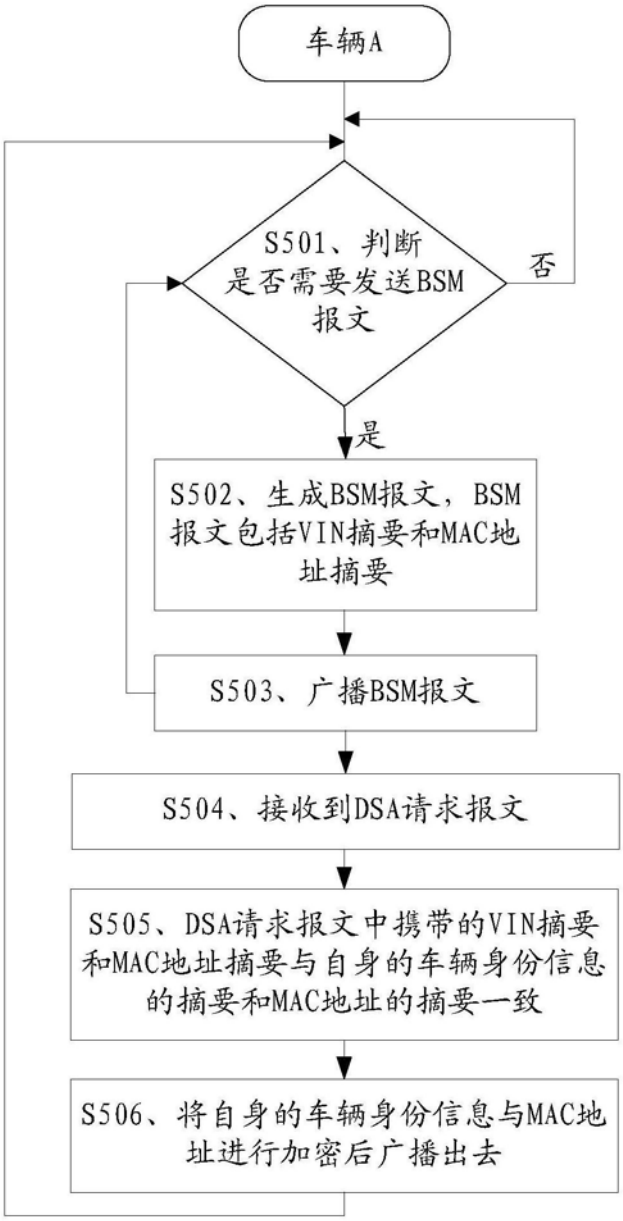

车辆A
S501、判断是否需要发送BSM报文
否
是
S502、生成BSM报文，BSM报文包括VIN摘要和MAC地址摘要
S503、广播BSM报文
S504、接收到DSA请求报文
S505、DSA请求报文中携带的VIN摘要和MAC地址摘要与自身的车辆身份信息的摘要和MAC地址的摘要一致
S506、将自身的车辆身份信息与MAC地址进行加密后广播出去

图5

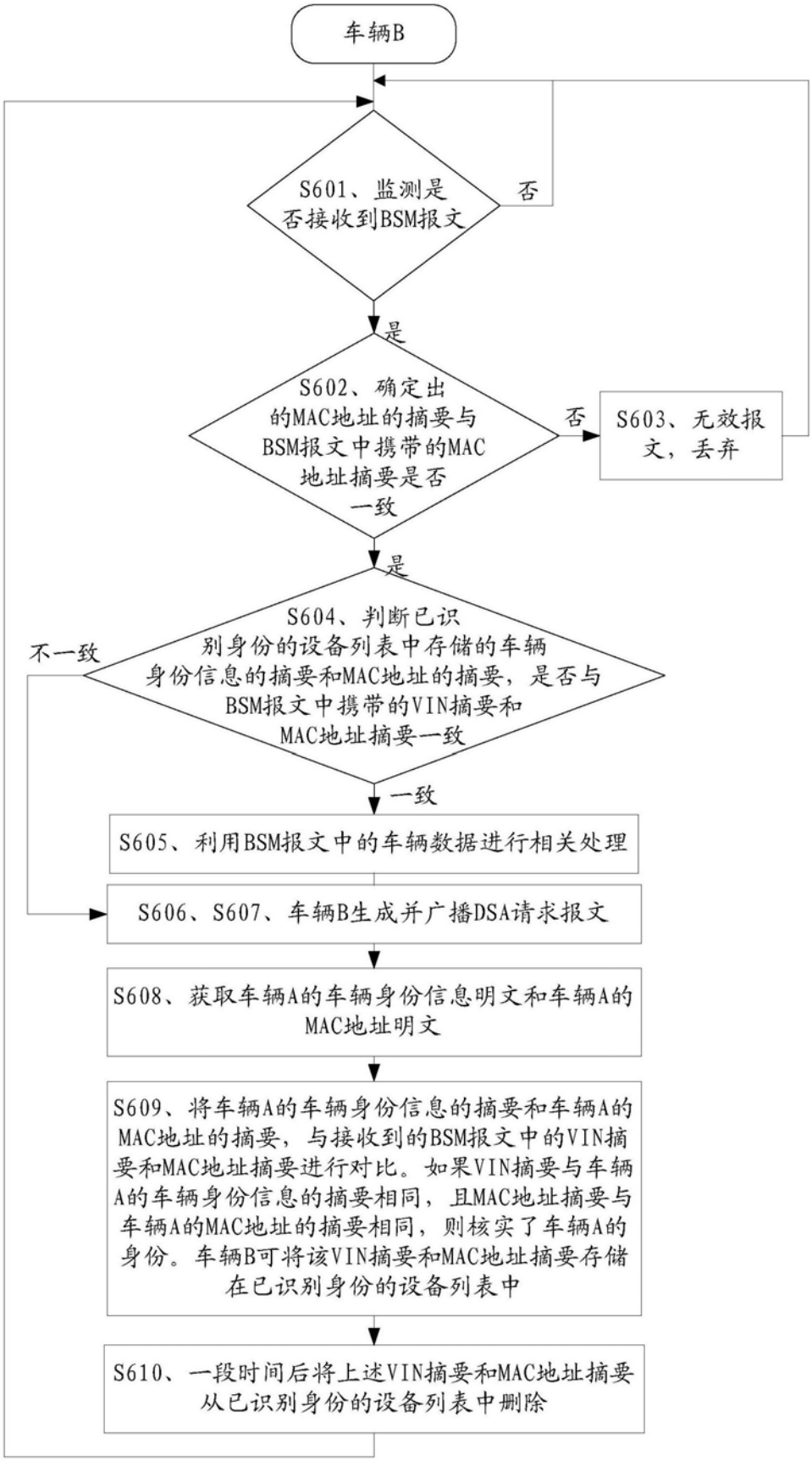

车辆B
S601、监测是否接收到BSM报文
否
是
S602、确定出的MAC地址的摘要与BSM报文中携带的MAC地址摘要是否一致
否
S603、无效报文，丢弃
是
S604、判断已识别身份的设备列表中存储的车辆身份信息的摘要和MAC地址的摘要，是否与BSM报文中携带的VIN摘要和MAC地址摘要一致
不一致
一致
S605、利用BSM报文中的车辆数据进行相关处理
S606、S607、车辆B生成并广播DSA请求报文
S608、获取车辆A的车辆身份信息明文和车辆A的MAC地址明文
S609、将车辆A的车辆身份信息的摘要和车辆A的MAC地址的摘要，与接收到的BSM报文中的VIN摘要和MAC地址摘要进行对比。如果VIN摘要与车辆A的车辆身份信息的摘要相同，且MAC地址摘要与车辆A的MAC地址的摘要相同，则核实了车辆A的身份。车辆B可将该VIN摘要和MAC地址摘要存储在已识别身份的设备列表中
S610、一段时间后将上述VIN摘要和MAC地址摘要从已识别身份的设备列表中删除

图6


接收设备
信息收发单元
接收单元701
发送单元705
综合逻辑处理单元
确定单元702
获取单元703
存储单元704

图7

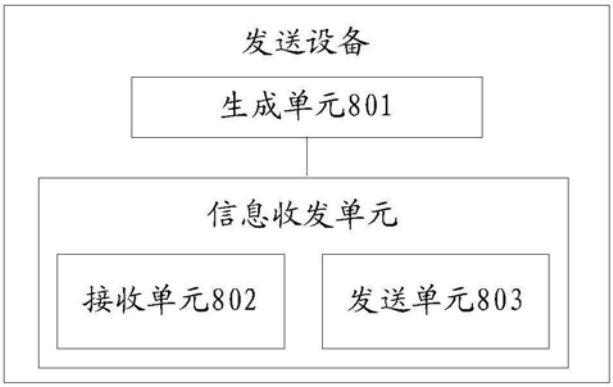

发送设备
生成单元801
信息收发单元
接收单元802
发送单元803

图8