(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 106792681 B
(45)授权公告日 2020.02.28

(21)申请号 201611070312.5

(22)申请日 2016.11.28

(65)同一申请的已公布的文献号
申请公布号 CN 106792681 A

(43)申请公布日 2017.05.31

(73)专利权人 北京梆梆安全科技有限公司
地址 100083 北京市海淀区学院路30号天工大厦A座20层

(72)发明人 阚志刚 卢佐华 叶威 彭建芬 陈彪

(74)专利代理机构 北京志霖恒远知识产权代理事务所(普通合伙) 11435
代理人 陈姗姗

(51)Int.Cl.
H04W 12/06(2009.01)
H04W 12/12(2009.01)
H04L 29/06(2006.01)

审查员 金凤

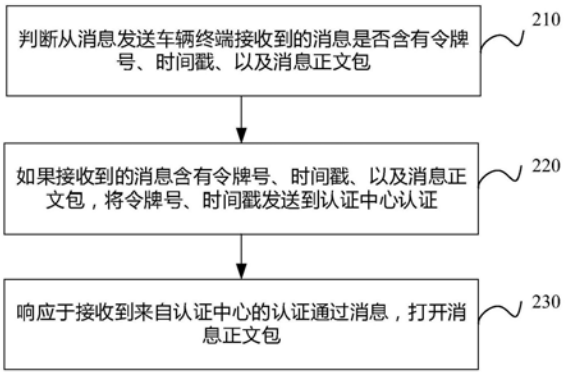
权利要求书4页 说明书11页 附图5页

(54)发明名称

用于车联网的入侵检测方法和装置及设备

(57)摘要

本申请公开了一种用于车联网的入侵检测方法和装置。所述方法包括:判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包;如果接收到的消息含有令牌号、时间戳、以及消息正文包,将令牌号、时间戳发送到认证中心认证,其中,所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放,时间戳表示发放所述令牌号的时间;响应于接收到来自认证中心的认证通过消息,打开消息正文包。本申请解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。



CN 106792681 B

1.一种用于车联网的入侵检测方法,其特征在于,应用于消息接收车辆终端,所述方法包括:

判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包,所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施;

如果接收到的消息含有令牌号、时间戳、以及消息正文包,将令牌号、时间戳发送到认证中心认证,以使所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对,其中,所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放,时间戳表示发放所述令牌号的时间;

响应于接收到来自认证中心的认证通过消息,打开消息正文包。

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:

如果接收到的消息不含有令牌号及时间戳,丢弃接收到的消息。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

响应于接收到来自认证中心的认证失败消息,丢弃接收到的消息。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

如果接收到的消息不含有令牌号及时间戳,或者接收到来自认证中心的认证失败消息,向安全中心发送报警消息。

5.一种用于车联网的入侵检测方法,其特征在于,应用于认证中心,所述方法包括:

从消息接收车辆终端接收令牌号和时间戳,其中,所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端,时间戳由认证中心发放,表示发放所述令牌号的时间,所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施;

将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比;

如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中,向消息接收车辆终端发送认证通过消息。

6.根据权利要求5所述的方法,其特征在于,所述方法还包括:

如果从消息接收车辆终端接收令牌号和时间戳不存在于发放的令牌号与时间戳对应记录之中,向消息接收车辆终端发送认证失败消息。

7.根据权利要求5所述的方法,其特征在于,所述方法在从消息接收车辆终端接收令牌号和时间戳之前还包括:

从消息发送车辆终端接收消息发送车辆终端的标识;

如果消息发送车辆终端是车联网注册车辆终端,生成令牌号;

将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。

8.根据权利要求7所述的方法,其特征在于,所述方法在将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端之后还包括:

将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录。

9.一种用于车联网的入侵检测方法,其特征在于,应用于消息发送车辆终端,所述方法包括:

向认证中心发送消息发送车辆终端的标识;

如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；

向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施，以使所述消息接收车辆终端将所述令牌号和时间戳发送给所述认证中心，以便所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对。

10.一种用于车联网的入侵检测装置，其特征在于，所述装置包括：

判断单元，配置用于判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施；

第一发送单元，配置用于如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，以使所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；

打开单元，配置用于响应于接收到来自认证中心的认证通过消息，打开消息正文包。

11.根据权利要求10所述的装置，其特征在于，所述装置还包括：

第一丢弃单元，配置用于如果接收到的消息不含有令牌号及时间戳，丢弃接收到的消息。

12.根据权利要求10所述的装置，其特征在于，所述装置还包括：

第二丢弃单元，配置用于响应于接收到来自认证中心的认证失败消息，丢弃接收到的消息。

13.根据权利要求10所述的装置，其特征在于，所述装置还包括：

第二发送单元，配置用于如果接收到的消息不含有令牌号及时间戳，或者接收到来自认证中心的认证失败消息，向安全中心发送报警消息。

14.一种用于车联网的入侵检测装置，其特征在于，所述装置包括：

第一接收单元，配置用于从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由认证中心发放，表示发放所述令牌号的时间，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施；

比对单元，配置用于将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行比对；

第三发送单元，配置用于如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

15.根据权利要求14所述的装置，其特征在于，所述装置还包括：

第四发送单元，配置用于如果从消息接收车辆终端接收令牌号和时间戳不存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证失败消息。

16.根据权利要求14所述的装置，其特征在于，所述装置还包括：

第五发送单元，配置用于从消息发送车辆终端接收消息发送车辆终端的标识；

生成单元，配置用于如果消息发送车辆终端是车联网注册车辆终端，生成令牌号；

发放单元，配置用于将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。

17.根据权利要求16所述的装置，其特征在于，所述装置还包括：

记录单元，配置用于在将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端之后，将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录。

18.一种用于车联网的入侵检测装置，其特征在于，所述装置包括：

第六发送单元，配置用于向认证中心发送消息发送车辆终端的标识；

第二接收单元，配置用于如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；

第七发送单元，配置用于向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施，以使所述消息接收车辆终端将所述令牌号和时间戳发送给所述认证中心，以便所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对。

19.一种计算机设备，包括处理器、存储器和显示器；其特征在于：

所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：

判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施；

如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，以使所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；

响应于接收到来自认证中心的认证通过消息，打开消息正文包。

20.一种计算机设备，包括处理器、存储器和显示器；其特征在于：

所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：

从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由认证中心发放，表示发放所述令牌号的时间，所述消息接收车辆终端包括车载单元和/或在道路两边铺设的网络基础设施；

将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比；

如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

21.一种计算机设备，包括处理器、存储器和显示器；其特征在于：

所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：

向认证中心发送消息发送车辆终端的标识；

如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；

向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息，所述消息接收

车辆终端包括车载单元和/或在道路两边铺设的网络基础设施，以使所述消息接收车辆终端将所述令牌号和时间戳发送给所述认证中心，以便所述认证中心将接收到的所述令牌号和所述时间戳与自身存储的令牌号和时间戳进行比对。

用于车联网的入侵检测方法和装置及设备

技术领域

[0001] 本公开一般涉及计算机技术领域，具体涉及网络信息安全领域，尤其涉及一种用于车联网的入侵检测方法和装置。

背景技术

[0002] 车联网是通过在车辆上装备可以无线通信的车载单元(OBU)，并在道路两边铺设网络基础设施(RSU)，实现车辆之间以及车辆和基础设施之间的协同通信而形成的车辆移动自组织网络，实现提高交通安全、优化交通效率、方便交通管理的目的。车联网中的车辆在没有网络基础设施的参与的情况下不断进行自我配置。车载单元每100-300毫秒向网络中广播道路交通相关和车辆自身状况等信标信息，包括车辆当前的位置、速度、交通状态等。

[0003] 但是，车联网中的车载单元(OBU)或网络基础设施(RSU)接收到的消息并不一定都是车联网中的其它车载单元发来的消息。有些非车联网注册用户的恶意用户向车联网中的车载单元发送带有病毒等的消息。车载单元接收到该消息后，打开消息，消息中的病毒迅速在车载单元中扩散，使车载单元不能正常工作，即入侵车载单元。

[0004] 因此，现有技术需要一种能够解决非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

发明内容

[0005] 鉴于现有技术中的上述缺陷或不足，期望提供一种能够解决非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0006] 第一方面，本申请实施例提供了一种用于车联网的入侵检测方法，所述方法包括：判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包；如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；响应于接收到来自认证中心的认证通过消息，打开消息正文包。

[0007] 第二方面，本申请实施例提供了一种用于车联网的入侵检测方法，所述方法包括：从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由消息发送车辆发放，表示发放所述令牌号的时间；将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比；如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

[0008] 第三方面，本申请实施例提供了一种用于车联网的入侵检测方法，所述方法包括：向认证中心发送消息发送车辆终端的标识；如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；向消息接收车辆终端

发送含有令牌号、时间戳、以及消息正文包的消息。

[0009] 第四方面，本申请实施例提供了一种用于车联网的入侵检测装置，所述装置包括：判断单元，配置用于判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包；第一发送单元，配置用于如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；打开单元，配置用于响应于接收到来自认证中心的认证通过消息，打开消息正文包。

[0010] 第五方面，本申请实施例提供了一种用于车联网的入侵检测装置，所述装置包括：第一接收单元，配置用于从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由消息发送车辆发放，表示发放所述令牌号的时间；比对单元，配置用于将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行比对；第三发送单元，配置用于如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

[0011] 第六方面，本申请实施例提供了一种用于车联网的入侵检测装置，所述装置包括：第六发送单元，配置用于向认证中心发送消息发送车辆终端的标识；第二接收单元，配置用于如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；第七发送单元，配置用于向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息。

[0012] 第七方面，本申请实施例提供了一种设备，包括处理器、存储器和显示器；所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包；如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；响应于接收到来自认证中心的认证通过消息，打开消息正文包。

[0013] 第八方面，本申请实施例提供了一种设备，包括处理器、存储器和显示器；所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由消息发送车辆发放，表示发放所述令牌号的时间；将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比；如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

[0014] 第九方面，本申请实施例提供了一种设备，包括处理器、存储器和显示器；所述存储器包含可由所述处理器执行的指令以使得所述处理器执行：向认证中心发送消息发送车辆终端的标识；如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息。

[0015] 在本申请实施例中，消息发送车辆终端要想发送车辆消息，首先请求认证中心为其发放令牌号和时间戳。该令牌号代表消息发送车辆终端有权向消息接收车辆终端发送消

息。认证中心认证其属于车联网注册车辆终端后，为其发放令牌号和时间戳。消息发送车辆终端将令牌号、时间戳、以及消息正文包一起发送给消息接收车辆终端。消息接收车辆终端不是立刻打开消息正文包，而是先判断伴随该消息正文包是否有令牌号和时间戳。如没有令牌号和时间戳，说明有可能是非车联网注册用户恶意向消息接收车辆终端发送带有病毒的消息。非车联网注册用户即使向认证中心请求发放令牌号和时间戳，由于其是非车联网注册用户，是拿不到令牌号和时间戳的，因而如果接收的消息没有令牌号和时间戳则不能打开消息正文包。另外，即使消息中含有令牌号和时间戳，也没有排除非车联网注册用户伪造令牌号和时间戳的可能。因此，消息发送车辆终端将令牌号和时间戳发送到认证中心，与认证中心发放令牌号和时间戳的记录进行比对，即认证。如认证失败，很有可能是非车联网注册用户伪造令牌号和时间戳恶意入侵的情况，不能打开消息正文包。只有当消息接收车辆终端接收到来自认证中心的认证通过消息，才能打开消息正文包。这样，就解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

附图说明

[0016] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0017] 图1示出了其中可以应用本申请实施例的示例性系统架构；

[0018] 图2示出了根据本申请一个实施例的在消息接收车辆终端侧的用于车联网的入侵检测方法的示例性流程图；

[0019] 图3示出了根据本申请一个实施例的在认证中心侧的用于车联网的入侵检测方法的示例性流程图；

[0020] 图4示出了根据本申请一个实施例的在消息发送车辆终端侧的用于车联网的入侵检测方法的示例性流程图；

[0021] 图5示出了根据本申请一个实施例的在消息接收车辆终端侧的用于车联网的入侵检测装置的示例性结构框图；

[0022] 图6示出了根据本申请一个实施例的在认证中心侧的用于车联网的入侵检测装置的示例性结构框图；

[0023] 图7示出了根据本申请一个实施例的在消息发送车辆终端侧的用于车联网的入侵检测装置的示例性结构框图；

[0024] 图8示出了适于用来实现本申请实施例的消息接收车辆终端的计算机系统的结构示意图。

[0025] 图9示出了适于用来实现本申请实施例的认证中心的计算机系统的结构示意图。

[0026] 图10示出了适于用来实现本申请实施例的消息发送车辆终端的计算机系统的结构示意图。

具体实施方式

[0027] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了

便于描述,附图中仅示出了与发明相关的部分。

[0028] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0029] 请参考图1,其示出了可以应用本申请实施例的示例性系统架构。

[0030] 如图1所示,系统架构可以包括消息发送车辆终端102、认证中心101、消息接收车辆终端103。消息发送车辆终端102指车联网中发送车辆消息的终端,一般指发送车辆消息的车载单元(OBU)。消息接收车辆终端103指车联网中接收车辆消息的终端,如接收车辆消息的车载单元(OBU)和网络基础设施(RSU)。一般地说,在作为消息发送车辆终端102的车载单元(OBU)广播道路交通相关和车辆自身状况等信标信息的情况下,车辆中所有的车载单元(OBU)和网络基础设施(RSU)都是消息接收车辆终端103。认证中心101指车联网中用于对车辆消息的发送者的身份进行安全认证的中心,防止不是车联网中注册的用户恶意向消息接收车辆终端发送带有病毒的消息、实现对车联网的入侵。

[0031] 消息发送车辆终端102、消息接收车辆终端103一般采用车载终端的形式,也可以采用用户携带的移动终端的形式。认证中心101可以包括一台或多条相互通信的服务器。

[0032] 如背景技术中提到的,有些非车联网注册用户的恶意用户向车联网中的车载单元发送带有病毒等的消息。车载单元接收到该消息后,打开消息,消息中的病毒迅速在车载单元中扩散,使车载单元不能正常工作,即入侵车载单元。因此,现有技术需要一种能够解决非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0033] 在本申请实施例中,消息发送车辆终端要想发送车辆消息,首先请求认证中心为其发放令牌号和时间戳。该令牌号代表消息发送车辆终端有权向消息接收车辆终端发送消息。认证中心认证其属于车联网注册车辆终端后,为其发放令牌号和时间戳。消息发送车辆终端将令牌号、时间戳、以及消息正文包一起发送给消息接收车辆终端。消息接收车辆终端不是立刻打开消息正文包,而是先判断伴随该消息正文包是否有令牌号和时间戳。如没有令牌号和时间戳,说明有可能是非车联网注册用户恶意向消息接收车辆终端发送带有病毒的消息。非车联网注册用户即使向认证中心请求发放令牌号和时间戳,由于其是非车联网注册用户,是拿不到令牌号和时间戳的,因而如果接收的消息没有令牌号和时间戳则不能打开消息正文包。另外,即使消息中含有令牌号和时间戳,也没有排除非车联网注册用户伪造令牌号和时间戳的可能。因此,消息发送车辆终端将令牌号和时间戳发送到认证中心,与认证中心发放令牌号和时间戳的记录进行比对,即认证。如认证失败,很有可能是非车联网注册用户伪造令牌号和时间戳恶意入侵的情况,不能打开消息正文包。只有当消息接收车辆终端接收到来自认证中心的认证通过消息,才能打开消息正文包。这样,就解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0034] 参考图2,其示出了根据本申请一个实施例的用于车联网的入侵检测方法的示例性流程图。图2所示的方法可以在图1中的消息接收车辆终端103执行。

[0035] 如图2所示,在步骤210中,判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包。

[0036] 消息发送车辆终端要想发送车辆消息,首先要请求认证中心为其发放令牌号和时

间戳。该令牌号代表消息发送车辆终端有权向消息接收车辆终端发送消息。这时，消息发送车辆终端需要向认证中心发送消息发送车辆终端的标识，以便认证中心认证。消息发送车辆终端的标识例如消息发送车辆的车牌号。车辆终端注册进车联网时，都将自己的终端标识备案在认证中心。这样，当认证中心接收到消息发送车辆终端的标识后，与备案的车辆终端标识进行比对。如果接收到的消息发送车辆终端的标识在备案的车辆终端标识中，认证通过，说明消息发送车辆终端是车联网注册车辆终端，认证中心生成令牌号。在一个实施例中，每次响应于接收到消息发送车辆终端的标识而生成的令牌号互不相同。然后，认证中心将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。在一个实施例中，认证中心需要将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录，以便在后续过程中认证中心将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳的对应记录进行对比。

[0037] 然后，消息发送车辆终端将消息正文包、以及从认证中心接收到的令牌号、时间戳一起发送给消息接收车辆终端。消息接收车辆终端接收后，不是立刻打开消息正文包，而是先判断伴随该消息正文包是否有令牌号和时间戳。

[0038] 在步骤220中，如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证。

[0039] 如果接收到的消息中没有令牌号和时间戳，说明有可能是非车联网注册用户恶意向消息接收车辆终端发送带有病毒的消息。非车联网注册用户即使向认证中心请求发放令牌号和时间戳，由于其是非车联网注册用户，是拿不到令牌号和时间戳的，因而如果接收的消息没有令牌号和时间戳则不能打开消息正文包。另外，即使消息中含有令牌号和时间戳，也没有排除非车联网注册用户伪造令牌号和时间戳的可能。因此，消息发送车辆终端将令牌号和时间戳发送到认证中心，与认证中心发放令牌号和时间戳的记录进行比对，即认证。

[0040] 由于认证中心将发放给消息发送车辆终端的令牌号和表示发放所述令牌号的时间的时间戳都对应地记录，因此，认证中心将从消息接收车辆终端接收到的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比。即，按照从消息接收车辆终端接收到的时间戳，查找记录中与该时间戳对应的令牌号中是否有该从消息接收车辆终端接收到的令牌号。如是，则认证通过，向消息接收车辆终端发送认证通过消息。反之，向消息接收车辆终端发送认证失败消息。

[0041] 在步骤230中，响应于接收到来自认证中心的认证通过消息，打开消息正文包。

[0042] 消息接收车辆终端如接收到认证失败消息，则很有可能是非车联网注册用户伪造令牌号和时间戳恶意入侵的情况，不能打开消息正文包。只有当消息接收车辆终端接收到来自认证中心的认证通过消息，才能打开消息正文包。这样，就解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0043] 在一个实施例中，所述方法还包括：如果接收到的消息不含有令牌号及时间戳，丢弃接收到的消息(未示)。

[0044] 在一个实施例中，所述方法还包括：响应于接收到来自认证中心的认证失败消息，丢弃接收到的消息(未示)。

[0045] 在一个实施例中，所述方法还包括：如果接收到的消息不含有令牌号及时间戳，或者接收到来自认证中心的认证失败消息，向安全中心发送报警消息(未示)。

[0046] 安全中心是车联网中负责安全维护的单元。向安全中心发送报警消息，有利于安全中心针对该接收到的消息不含有令牌号及时间戳、或者接收到来自认证中心的认证失败消息的情形展开进一步的分析，采取进一步的措施，消除安全隐患。

[0047] 参考图3，其示出了根据本申请一个实施例的用于车联网的入侵检测方法的示例性流程图。图3所示的方法可以在图1中的认证中心101执行。

[0048] 如图3所示，在步骤310中，从消息接收车辆终端接收令牌号和时间戳。所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端。时间戳由消息发送车辆发放，表示发放所述令牌号的时间。

[0049] 实际上，在步骤310之前，认证中心还执行以下的过程：从消息发送车辆终端接收消息发送车辆终端的标识；如果消息发送车辆终端是车联网注册车辆终端，生成令牌号；将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。

[0050] 消息发送车辆终端要想发送车辆消息，首先要请求认证中心为其发放令牌号和时间戳。该令牌号代表消息发送车辆终端有权向消息接收车辆终端发送消息。这时，消息发送车辆终端需要向认证中心发送消息发送车辆终端的标识，以便认证中心认证。消息发送车辆终端的标识例如消息发送车辆的车牌号。车辆终端注册进车联网时，都将自己的终端标识备案在认证中心。这样，当认证中心接收到消息发送车辆终端的标识后，与备案的车辆终端标识进行比对。如果接收到的消息发送车辆终端的标识在备案的车辆终端标识中，认证通过，说明消息发送车辆终端是车联网注册车辆终端，认证中心生成令牌号。在一个实施例中，每次响应于接收到消息发送车辆终端的标识而生成的令牌号互不相同。然后，认证中心将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。在一个实施例中，认证中心需要将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录，以便在后续步骤320中认证中心将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳的对应记录进行对比。

[0051] 然后，消息发送车辆终端将消息正文包、以及从认证中心接收到的令牌号、时间戳一起发送给消息接收车辆终端。消息接收车辆终端接收后，不是立刻打开消息正文包，而是先判断伴随该消息正文包是否有令牌号和时间戳。如果接收到的消息中没有令牌号和时间戳，说明有可能是非车联网注册用户恶意向消息接收车辆终端发送带有病毒的消息。非车联网注册用户即使向认证中心请求发放令牌号和时间戳，由于其是非车联网注册用户，是拿不到令牌号和时间戳的，因而如果接收的消息没有令牌号和时间戳则不能打开消息正文包。另外，即使消息中含有令牌号和时间戳，也没有排除非车联网注册用户伪造令牌号和时间戳的可能。因此，消息发送车辆终端将令牌号和时间戳发送到认证中心，与认证中心发放令牌号和时间戳的记录进行比对，即认证。

[0052] 在步骤320中，将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比。

[0053] 由于认证中心将发放给消息发送车辆终端的令牌号和表示发放所述令牌号的时间的时间戳都对应地记录，因此，认证中心能够将从消息接收车辆终端接收到的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比。即，认证中心按照从消息接收车辆终端接收到的时间戳，查找记录中与该时间戳对应的令牌号中是否有该从消息接收车辆终端接收到的令牌号。如是，则认证通过，反之，则认证失败。

[0054] 在步骤330中，如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

[0055] 即，在认证通过的情况下，认证中心向消息接收车辆终端发送认证通过消息。

[0056] 在一个实施例中，所述方法还包括：如果从消息接收车辆终端接收令牌号和时间戳不存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证失败消息(未示)。

[0057] 即，在认证失败的情况下，认证中心向消息接收车辆终端发送认证失败消息。

[0058] 消息接收车辆终端如接收到认证失败消息，则很有可能是非车联网注册用户伪造令牌号和时间戳恶意入侵的情况，不能打开消息正文包。只有当消息接收车辆终端接收到来自认证中心的认证通过消息，才能打开消息正文包。这样，就解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0059] 参考图4，其示出了根据本申请一个实施例的用于车联网的入侵检测方法的示例性流程图。图3所示的方法可以在图1中的消息发送车辆终端102执行。

[0060] 如图4所示，在步骤410中，向认证中心发送消息发送车辆终端的标识。

[0061] 消息发送车辆终端要想发送车辆消息，首先要请求认证中心为其发放令牌号和时间戳。该令牌号代表消息发送车辆终端有权向消息接收车辆终端发送消息。这时，消息发送车辆终端需要向认证中心发送消息发送车辆终端的标识，以便认证中心认证。消息发送车辆终端的标识例如消息发送车辆的车牌号。

[0062] 在步骤420中，如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳。

[0063] 车辆终端注册进车联网时，都将自己的终端标识备案在认证中心。这样，当认证中心接收到消息发送车辆终端的标识后，与备案的车辆终端标识进行比对。如果接收到的消息发送车辆终端的标识在备案的车辆终端标识中，认证通过，说明消息发送车辆终端是车联网注册车辆终端，认证中心生成令牌号。在一个实施例中，每次响应于接收到消息发送车辆终端的标识而生成的令牌号互不相同。然后，认证中心将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。在一个实施例中，认证中心需要将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录，以便在后续过程中认证中心将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳的对应记录进行对比。

[0064] 在步骤430中，向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息。

[0065] 即，消息发送车辆终端将消息正文包、以及从认证中心接收到的令牌号、时间戳一起发送给消息接收车辆终端。消息接收车辆终端接收后，不是立刻打开消息正文包，而是先判断伴随该消息正文包是否有令牌号和时间戳。如果接收到的消息中没有令牌号和时间戳，说明有可能是非车联网注册用户恶意向消息接收车辆终端发送带有病毒的消息。非车联网注册用户即使向认证中心请求发放令牌号和时间戳，由于其是非车联网注册用户，是拿不到令牌号和时间戳的，因而如果接收的消息没有令牌号和时间戳则不能打开消息正文包。另外，即使消息中含有令牌号和时间戳，也没有排除非车联网注册用户伪造令牌号和时间戳的可能。因此，消息发送车辆终端将令牌号和时间戳发送到认证中心，与认证中心发放

令牌号和时间戳的记录进行比对，即认证。

[0066] 由于认证中心将发放给消息发送车辆终端的令牌号和表示发放所述令牌号的时间的时间戳都对应地记录，因此，认证中心能够将从消息接收车辆终端接收到的令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比。即，认证中心按照从消息接收车辆终端接收到的时间戳，查找记录中与该时间戳对应的令牌号中是否有该从消息接收车辆终端接收到的令牌号。如是，则认证通过，反之，则认证失败。在认证通过的情况下，认证中心向消息接收车辆终端发送认证通过消息。在认证失败的情况下，认证中心向消息接收车辆终端发送认证失败消息。

[0067] 消息接收车辆终端如接收到认证失败消息，则很有可能是非车联网注册用户伪造令牌号和时间戳恶意入侵的情况，不能打开消息正文包。只有当消息接收车辆终端接收到来自认证中心的认证通过消息，才能打开消息正文包。这样，就解决了非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息、实现对车联网的入侵的问题。

[0068] 应当注意，尽管在附图中以特定顺序描述了本发明方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。相反，流程图中描绘的步骤可以改变执行顺序。附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个步骤执行。

[0069] 进一步参考图5，其示出了根据本申请一个实施例的用于车联网的入侵检测装置500的示例性结构框图。

[0070] 如图5所示，用于车联网的入侵检测装置500可以包括：判断单元510，配置用于判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包；第一发送单元520，配置用于如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放，时间戳表示发放所述令牌号的时间；打开单元530，配置用于响应于接收到来自认证中心的认证通过消息，打开消息正文包。

[0071] 可选地，所述装置500还包括：第一丢弃单元(未示)，配置用于如果接收到的消息不含有令牌号及时间戳，丢弃接收到的消息。

[0072] 可选地，所述装置500还包括：第二丢弃单元(未示)，配置用于响应于接收到来自认证中心的认证失败消息，丢弃接收到的消息。

[0073] 可选地，所述装置500还包括：第二发送单元(未示)，配置用于如果接收到的消息不含有令牌号及时间戳，或者接收到来自认证中心的认证失败消息，向安全中心发送报警消息。

[0074] 进一步参考图6，其示出了根据本申请一个实施例的用于车联网的入侵检测装置600的示例性结构框图。

[0075] 如图6所示，用于车联网的入侵检测装置600可以包括：第一接收单元610，配置用于从消息接收车辆终端接收令牌号和时间戳，其中，所述令牌号由消息发送车辆终端在需要发送消息时向认证中心请求发放并由消息发送车辆终端发送到消息接收车辆终端，时间戳由消息发送车辆发放，表示发放所述令牌号的时间；比对单元620，配置用于将从消息接收车辆终端接收的令牌号和时间戳与发放的令牌号与时间戳对应记录进行比对；第三发送单元630，配置用于如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与

时间戳对应记录之中，向消息接收车辆终端发送认证通过消息。

[0076] 可选地，所述装置600还包括：第四发送单元(未示)，配置用于如果从消息接收车辆终端接收令牌号和时间戳不存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证失败消息。

[0077] 可选地，所述装置600还包括：第五发送单元(未示)，配置用于从消息发送车辆终端接收消息发送车辆终端的标识；生成单元(未示)，配置用于如果消息发送车辆终端是车联网注册车辆终端，生成令牌号；发放单元(未示)，配置用于将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端。

[0078] 可选地，所述装置600还包括：记录单元(未示)，配置用于在将所述令牌号和表示发放所述令牌号的时间的时间戳发放给消息发送车辆终端之后，将发送的令牌号和表示发放所述令牌号的时间的时间戳对应地记录。

[0079] 进一步参考图7，其示出了根据本申请一个实施例的用于车联网的入侵检测装置700的示例性结构框图。

[0080] 如图7所示，用于车联网的入侵检测装置700可以包括：第六发送单元710，配置用于向认证中心发送消息发送车辆终端的标识；第二接收单元720，配置用于如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳；第七发送单元730，配置用于向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息。

[0081] 应当理解，图5-7中记载的诸子系统或单元与参考图2-图4描述的方法中的各个步骤相对应。由此，上文针对方法描述的操作和特征同样适用于图5-7及其中包含的单元，在此不再赘述。

[0082] 下面参考图8，其示出了适于用来实现本申请实施例的消息接收车辆终端的计算机系统800的结构示意图。

[0083] 如图8所示，计算机系统800包括中央处理单元(CPU)801，其可以根据存储在只读存储器(ROM)802中的程序或者从存储部分808加载到随机访问存储器(RAM)803中的程序而执行各种适当的动作和处理。在RAM 803中，还存储有系统800操作所需的各种程序和数据。CPU 801、ROM 802以及RAM 803通过总线804彼此相连。输入/输出(I/O)接口805也连接至总线804。

[0084] 以下部件连接至I/O接口805：包括键盘、鼠标等的输入部分806；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分807；包括硬盘等的存储部分808；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分809。通信部分809经由诸如因特网的网络执行通信处理。驱动器810也根据需要连接至I/O接口805。可拆卸介质811，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器810上，以便于从其上读出的计算机程序根据需要被安装入存储部分808。

[0085] 下面参考图9，其示出了适于用来实现本申请实施例的认证中心的计算机系统900的结构示意图。

[0086] 如图9所示，计算机系统900包括中央处理单元(CPU)901，其可以根据存储在只读存储器(ROM)902中的程序或者从存储部分908加载到随机访问存储器(RAM)903中的程序而执行各种适当的动作和处理。在RAM 903中，还存储有系统900操作所需的各种程序和数据。

CPU 901、ROM 902以及RAM 903通过总线904彼此相连。输入/输出(I/O)接口905也连接至总线904。

[0087] 以下部件连接至I/O接口905：包括键盘、鼠标等的输入部分906；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分907；包括硬盘等的存储部分908；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分909。通信部分909经由诸如因特网的网络执行通信处理。驱动器910也根据需要连接至I/O接口905。可拆卸介质911，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器910上，以便于从其上读出的计算机程序根据需要被安装入存储部分908。

[0088] 下面参考图10，其示出了适于用来实现本申请实施例的消息接收车辆终端的计算机系统1000的结构示意图。

[0089] 如图10所示，计算机系统1000包括中央处理单元(CPU)1001，其可以根据存储在只读存储器(ROM)1002中的程序或者从存储部分1008加载到随机访问存储器(RAM)1003中的程序而执行各种适当的动作和处理。在RAM 1003中，还存储有系统1000操作所需的各种程序和数据。CPU 1001、ROM 1002以及RAM 1003通过总线1004彼此相连。输入/输出(I/O)接口1005也连接至总线1004。

[0090] 以下部件连接至I/O接口1005：包括键盘、鼠标等的输入部分1006；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分1007；包括硬盘等的存储部分1008；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分1009。通信部分1009经由诸如因特网的网络执行通信处理。驱动器1010也根据需要连接至I/O接口1005。可拆卸介质1011，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器1010上，以便于从其上读出的计算机程序根据需要被安装入存储部分1008。

[0091] 特别地，根据本公开的实施例，上文参考图2-图4描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，所述计算机程序包含用于执行图2-图4的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分809、909、1009从网络上被下载和安装，和/或从可拆卸介质811、911、1011被安装。

[0092] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0093] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中。这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0094] 作为另一方面，本申请还提供了一种计算机可读存储介质，该计算机可读存储介

质可以是上述实施例中所述装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,所述程序被一个或者一个以上的处理器用来执行描述于本申请的公式输入方法。

[0095] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离所述发明构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

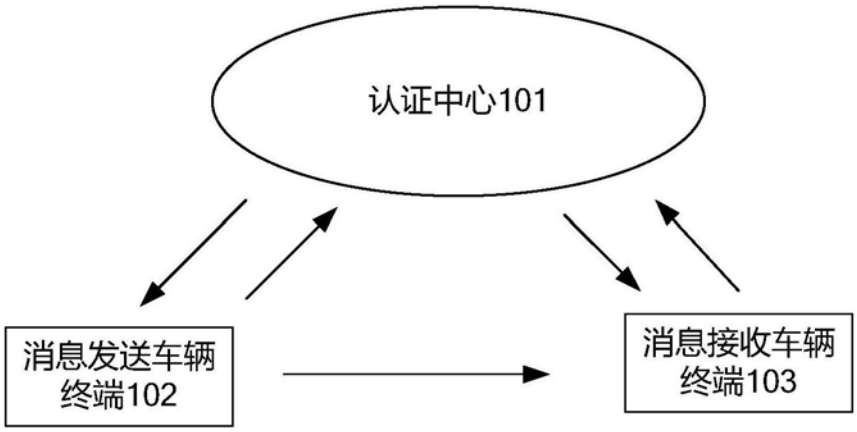

认证中心101
消息发送车辆终端102
消息接收车辆终端103

图1

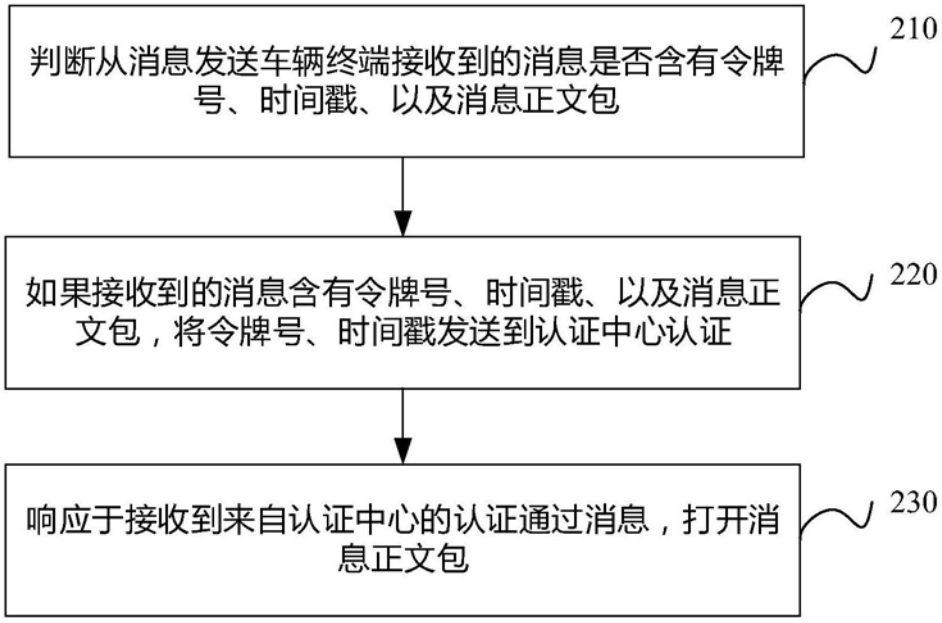

判断从消息发送车辆终端接收到的消息是否含有令牌号、时间戳、以及消息正文包
210
如果接收到的消息含有令牌号、时间戳、以及消息正文包，将令牌号、时间戳发送到认证中心认证
220
响应于接收到来自认证中心的认证通过消息，打开消息正文包
230

图2

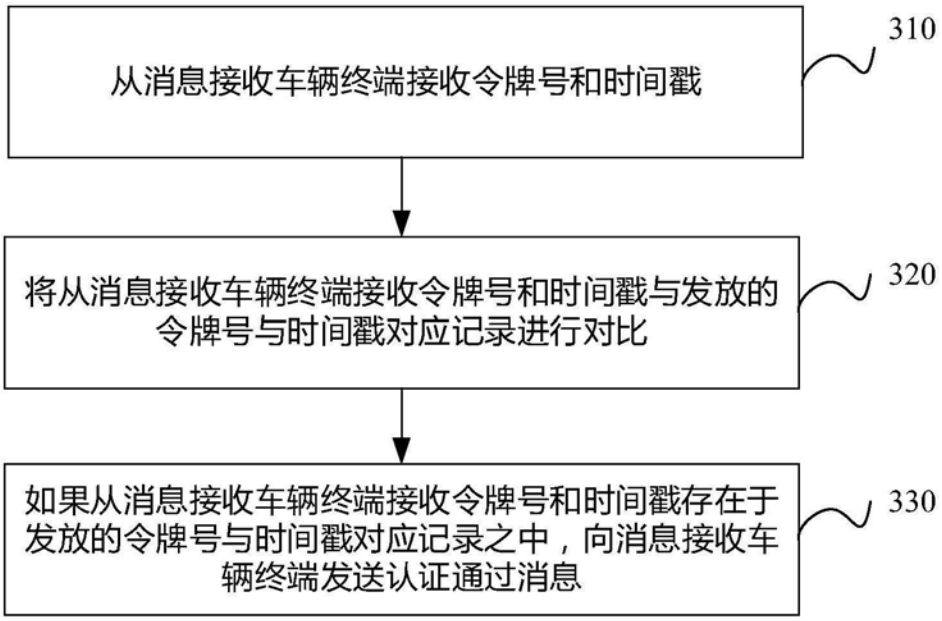

从消息接收车辆终端接收令牌号和时间戳
310
将从消息接收车辆终端接收令牌号和时间戳与发放的令牌号与时间戳对应记录进行对比
320
如果从消息接收车辆终端接收令牌号和时间戳存在于发放的令牌号与时间戳对应记录之中，向消息接收车辆终端发送认证通过消息
330

图3

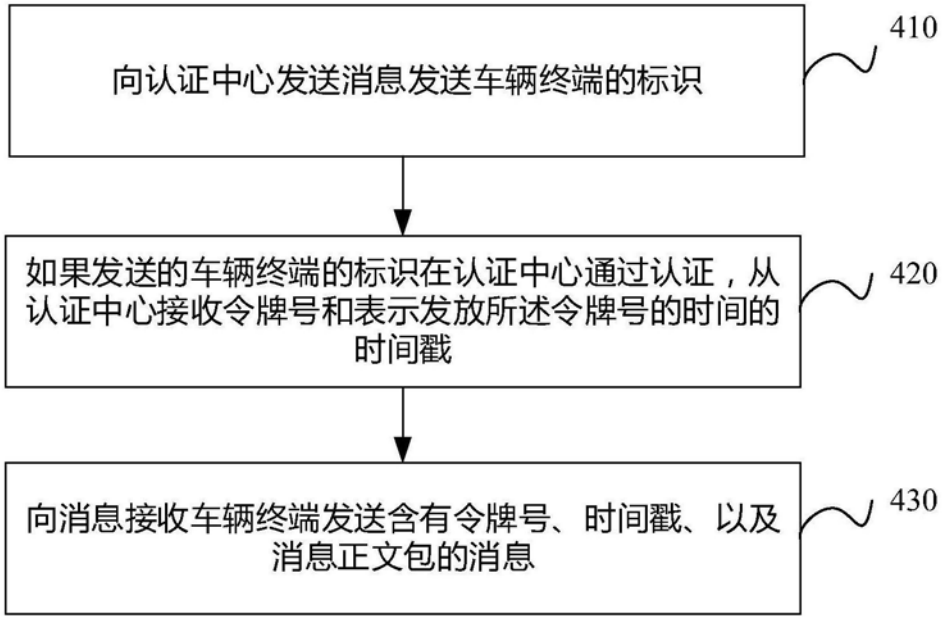

向认证中心发送消息发送车辆终端的标识
410
如果发送的车辆终端的标识在认证中心通过认证，从认证中心接收令牌号和表示发放所述令牌号的时间的时间戳
420
向消息接收车辆终端发送含有令牌号、时间戳、以及消息正文包的消息
430

图4

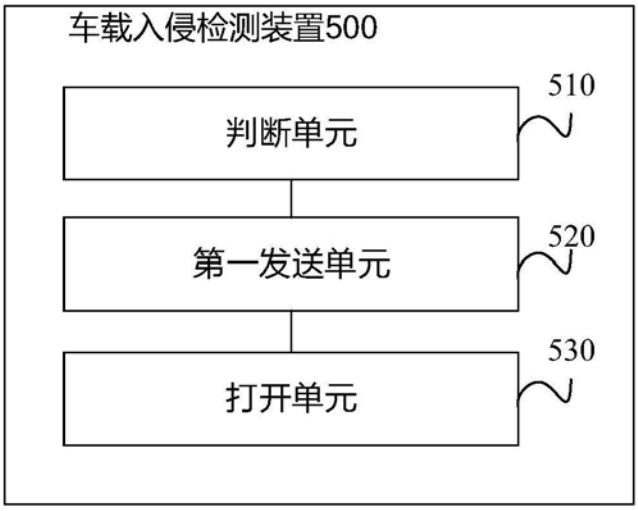

车载入侵检测装置500
判断单元
510
第一发送单元
520
打开单元
530

图5

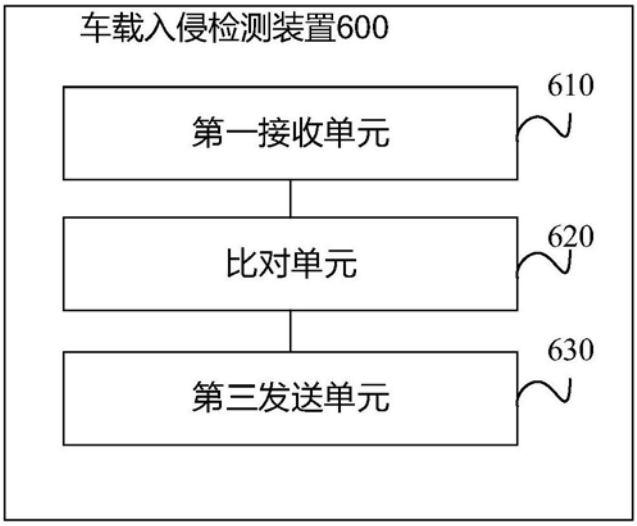

车载入侵检测装置600
第一接收单元
610
比对单元
620
第三发送单元
630

图6

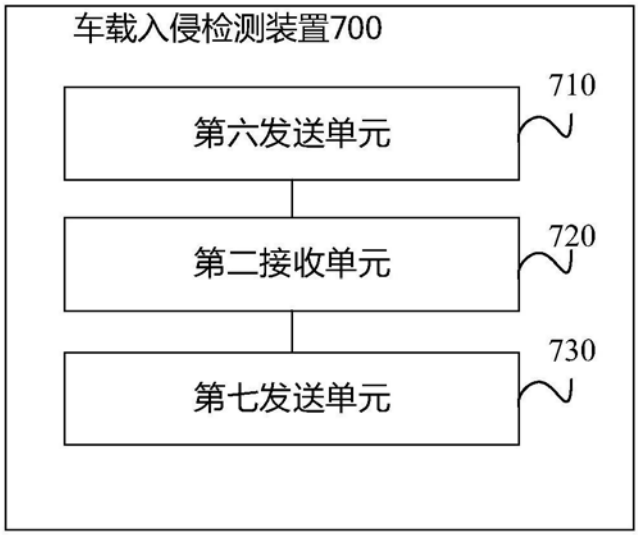

车载入侵检测装置700
710
第六发送单元
720
第二接收单元
730
第七发送单元

图7

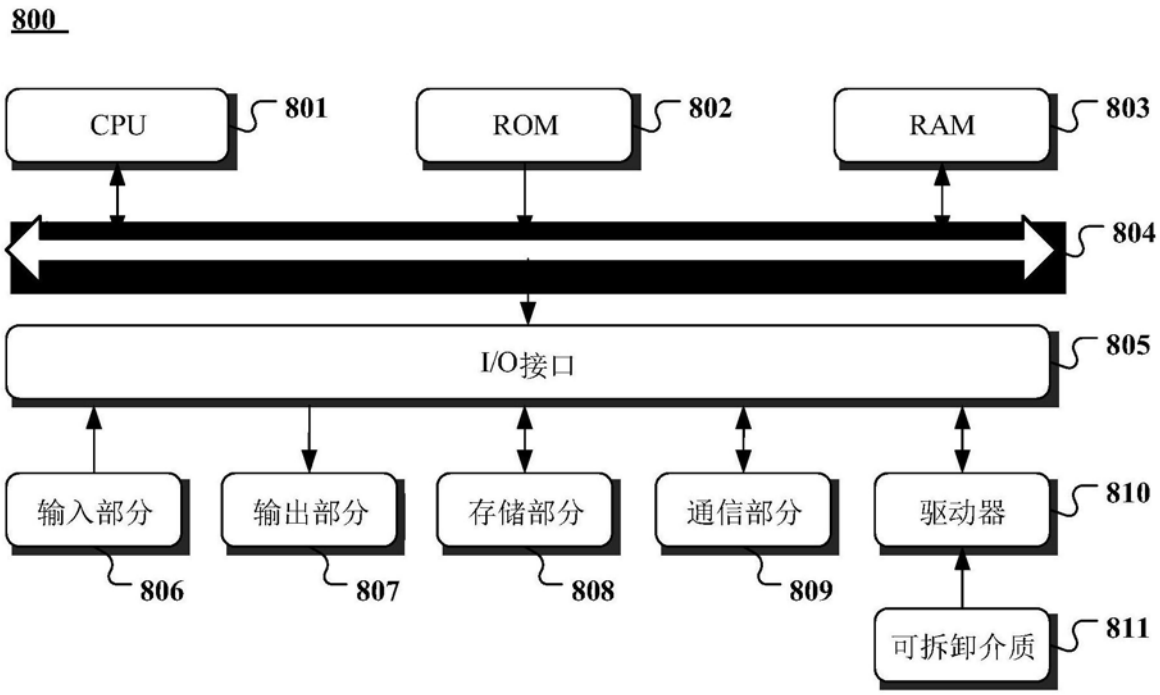

800
CPU
801
ROM
802
RAM
803
804
I/O接口
805
输入部分
806
输出部分
807
存储部分
808
通信部分
809
驱动器
810
可拆卸介质
811

图8

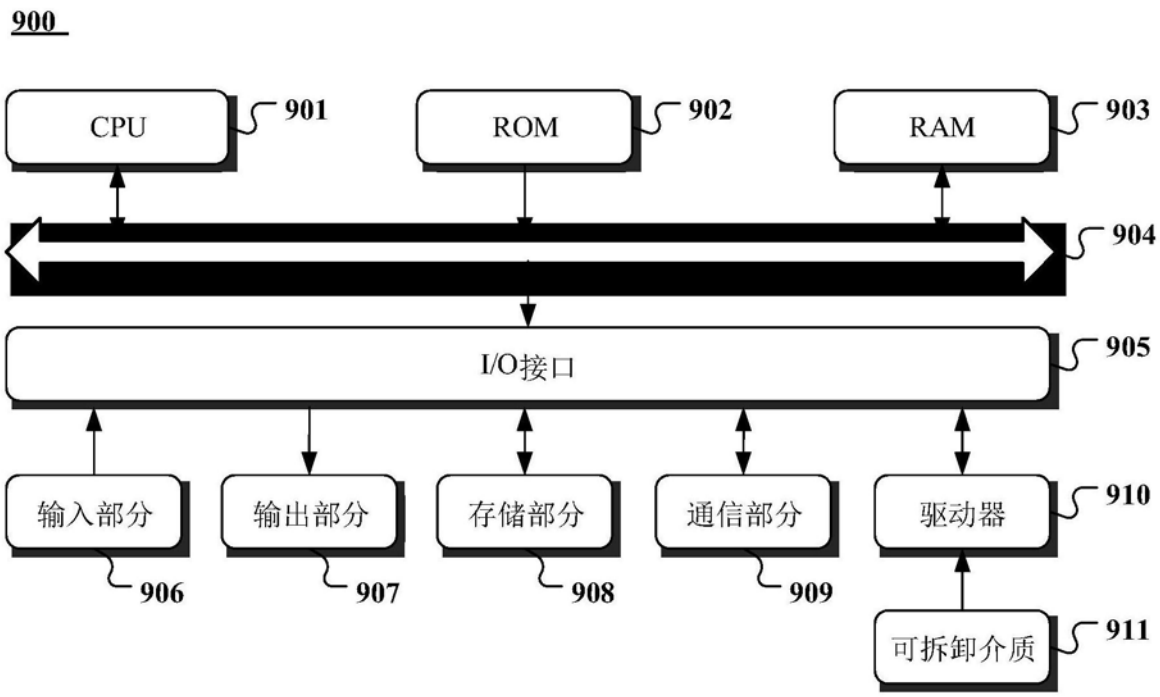

900
CPU
901
ROM
902
RAM
903
904
I/O接口
905
输入部分
906
输出部分
907
存储部分
908
通信部分
909
驱动器
910
可拆卸介质
911

图9

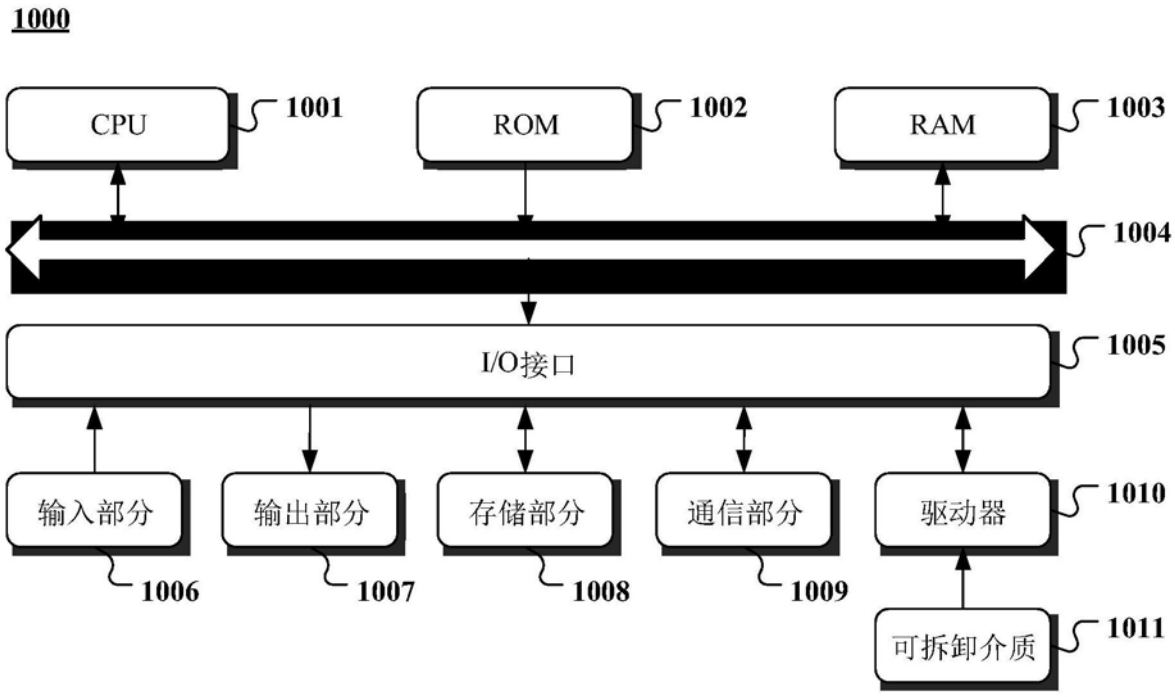

1000
CPU
1001
ROM
1002
RAM
1003
1004
I/O接口
1005
输入部分
1006
输出部分
1007
存储部分
1008
通信部分
1009
驱动器
1010
可拆卸介质
1011

图10