(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109547972 B
(45)授权公告日 2022.06.17

(21)申请号 201711238129.6
(22)申请日 2017.11.30
(65)同一申请的已公布的文献号
申请公布号 CN 109547972 A
(43)申请公布日 2019.03.29
(30)优先权数据
10-2017-0122721 2017.09.22 KR
(73)专利权人 现代自动车株式会社
地址 韩国首尔
专利权人 起亚自动车株式会社
高丽大学校产学协力团
(72)发明人 鲁东奎 成修莲 黄大成 朴钟录 卢鹤烈 柳初珑 李太俊 金孝坤 朴龙泰 安仁先 金泰镐
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
专利代理师 陈鹏 李静
(51)Int.Cl.
H04W 4/40(2018.01)
H04W 12/069(2021.01)
(56)对比文件
WO 2014171734 A2,2014.10.23
KR 101714525 B1,2017.03.22
EP 2945137 A1,2015.11.18
王良民等.基于车辆身份的车联网结构与安全.《网络与信息安全学报》.2016,(第02期),
须超等.车联网网络架构与媒质接入机制研究.《中兴通讯技术》.2011,(第03期),
审查员 张芃

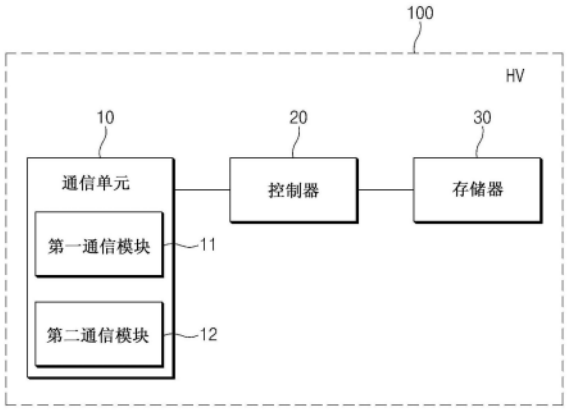
权利要求书2页 说明书9页 附图4页

(54)发明名称

用于在车辆间通信环境中验证车辆的方法和装置

(57)摘要

一种用于在车辆间通信环境中验证车辆的装置,包括:通信单元,被配置为从允许参与车辆间通信的远程车辆接收基本安全消息和验证消息;以及控制器,被配置为当通信单元在预定时间段内从远程车辆接收到至少预定次数的验证消息时,确定远程车辆是可靠的,并且当控制器确定远程车辆可靠时,生成许可以利用从远程车辆接收的基本安全消息。



CN 109547972 B

1.一种用于在车辆间通信环境中验证车辆的装置,所述装置包括:

第一通信模块,被配置为基于车载环境无线接入(WAVE)通信方案从被允许参与车辆间通信的远程车辆接收基本安全消息;

第二通信模块,被配置为基于选自由以下各项的组成的组中的短程通信方案从所述远程车辆接收验证消息:蓝牙、射频识别(RFID)、红外数据组织(IrDA)、超宽带(UWB)、ZigBee、近场通信(NFC)、无线保真(Wi-Fi)、Wi-Fi直连、无线通用串行总线(USB);以及

控制器,被配置为当所述第二通信模块在预定时间段内从所述远程车辆接收到至少预定次数的所述验证消息时,确定所述远程车辆是可靠的,并且当所述控制器确定所述远程车辆可靠时,所述控制器被配置为生成对于利用从所述远程车辆接收的所述基本安全消息的许可。

2.根据权利要求1所述的装置,其中,从所述远程车辆接收的所述验证消息包括所述远程车辆的证书摘要、所述远程车辆的唯一编号、以及所述远程车辆的唯一编号接收列表。

3.根据权利要求2所述的装置,其中,所述控制器还被配置为生成第二验证消息,以及控制所述第二通信模块将所生成的第二验证消息发送至所述远程车辆,其中,所述第二验证消息包括主车辆的唯一编号接收列表、所述主车辆的证书摘要、以及所述主车辆的唯一编号。

4.根据权利要求3所述的装置,其中,所述控制器还被配置为基于从所述远程车辆接收的包括所述主车辆的唯一编号的验证消息的次数,确定所述远程车辆是否可靠。

5.根据权利要求4所述的装置,其中,所述控制器还被配置为基于从所述远程车辆接收的包括所述主车辆的唯一编号的所述验证消息的次数,生成信任得分,并且当所计算的信任得分超过阈值得分时,确定所述远程车辆是可靠的。

6.根据权利要求5所述的装置,其中,所述控制器还被配置为匹配所述远程车辆的证书摘要、所述远程车辆的唯一编号、以及所述远程车辆的信任得分,以及将匹配的结果记录在所述第二验证消息的唯一编号接收列表。

7.根据权利要求5所述的装置,其中,所述控制器还可以被配置为每秒钟从所计算的信任得分减去预定得分。

8.根据权利要求3所述的装置,其中,所述第二通信模块还可以被配置为基于短程无线通信来发送所述第二验证消息。

9.根据权利要求3所述的装置,其中,所述第二验证消息的发送距离短于第二基本安全消息的发送距离,并且所述第二验证消息的发送周期长于所述第二基本安全消息的发送周期。

10.一种用于在车辆间通信环境中验证车辆的方法,所述方法包括以下步骤:

由第一通信模块基于车载环境无线接入(WAVE)通信方案从被允许参与车辆间通信的远程车辆接收基本安全消息;

由第二通信模块基于选自由以下各项的组成的组中的短程通信方案从所述远程车辆接收验证消息:蓝牙、射频识别(RFID)、红外数据组织(IrDA)、超宽带(UWB)、ZigBee、近场通信(NFC)、无线保真(Wi-Fi)、Wi-Fi直连、无线通用串行总线(USB);

当所述第二通信模块在预定时间段内从所述远程车辆接收到至少预定次数的所述验证消息时,由控制器确定所述远程车辆是可靠的;以及

由所述控制器生成对于利用从所述远程车辆接收的所述基本安全消息的许可。

11.根据权利要求10所述的方法，其中，从所述远程车辆接收的所述验证消息包括所述远程车辆的证书摘要、所述远程车辆的唯一编号、以及所述远程车辆的唯一编号接收列表。

12.根据权利要求11所述的方法，其中，确定所述远程车辆是可靠的，包括：

由所述控制器生成第二验证消息，其中，所述第二验证消息包括主车辆的唯一编号接收列表、所述主车辆的证书摘要、以及所述主车辆的唯一编号；以及

由所述控制器控制所述第二通信模块将所生成的第二验证消息发送到所述远程车辆。

13.根据权利要求12所述的方法，其中，确定所述远程车辆是可靠的，还包括：

由所述控制器基于从所述远程车辆接收的包括所述主车辆的唯一编号的验证消息的次数，确定所述远程车辆是否可靠。

14.根据权利要求13所述的方法，其中，确定所述远程车辆是可靠的，还包括：

由所述控制器基于从所述远程车辆接收的、包括所述主车辆的唯一编号的所述验证消息的次数，生成信任得分；以及

当所计算的信任得分超过阈值得分时，由所述控制器确定所述远程车辆是可靠的。

15.根据权利要求14所述的方法，其中，确定所述远程车辆是可靠的，还包括：

由所述控制器匹配所述远程车辆的证书摘要、所述远程车辆的唯一编号、以及所述远程车辆的信任得分；以及

由所述控制器将匹配的结果记录在所述第二验证消息的唯一编号接收列表中。

16.根据权利要求14所述的方法，还包括：由所述控制器每秒钟从所计算的信任得分减去预定得分。

17.根据权利要求12所述的方法，其中，所述第二验证消息是基于短程无线通信发送的。

18.根据权利要求12所述的方法，其中，所述第二验证消息的发送距离短于第二基本安全消息的发送距离，并且所述第二验证消息的发送周期长于所述第二基本安全消息的发送周期。

用于在车辆间通信环境中验证车辆的方法和装置

[0001] 相关申请的交叉引用

[0002] 本申请要求于2017年9月22日向韩国知识产权局提交的韩国专利申请第10-2017-0122721号的优先权,其公开内容通过引用整体并入本文。

技术领域

[0003] 本公开涉及用于在车辆间通信环境中验证车辆的方法和装置,并且更具体地说,涉及在车辆间通信环境中,通过使用基于短程无线通信的验证消息来确定远程车辆的可信度的技术。

背景技术

[0004] V2X(车到一切,Vehicle to Everything)通信包括V2V(车到车)无线通信、V2I(车到基础设施)无线通信、IVN(车载网络)和V2P(车到行人)通信。IEEE 1609.2是V2X无线通信标准之一,其定义安全框架。IEEE 1609.2的安全框架定义了使用对称密钥和非对称密钥以及通过验证消息发送过程的完整性来验证(在车辆中)发射器的过程。

[0005] IEEE 1609.2中的验证是给出参与车辆间通信的资格以及不处理确定消息(包含从有资格参与车辆间通信的车辆发送的车辆信息)的可信性的过程。因此,当允许车辆参与车辆间通信时,不可能确定通过在IEEE 1609.2中定义的验证过程的车辆发送的消息是否可信。

[0006] 换句话说,传统的车辆间通信环境中的车辆验证技术仅允许或禁止车辆间通信,但不能确定被允许车辆间通信的车辆所发送的车辆信息是否可信。

发明内容

[0007] 本公开旨在解决现有技术的上述问题。本公开提供用于在车辆间通信环境中验证车辆的方法和装置,在该方法和装置中,通过使用基于短程无线通信的验证消息验证远程车辆,可以确定被允许车辆间通信的车辆所发送的信息是否可信。

[0008] 本公开的目的不限于上述目的,并且本公开的其他未提及的目的和优点将通过以下描述来理解,并且将通过本公开的实施方式清楚地理解。此外,要注意的是,本公开的目的和优点将通过权利要求书中描述的手段及其组合来实现。

[0009] 根据本公开的实施方式,用于在车辆间通信环境中验证车辆的装置包括:通信单元,被配置为从允许参与车辆间通信的远程车辆接收基本安全消息和验证消息;以及控制器,被配置为当通信单元在预定时间段内从远程车辆接收到至少预定次数的验证消息时,确定远程车辆是可靠的,并且当控制器确定远程车辆可靠时,生成许可以利用从远程车辆接收的基本安全消息。

[0010] 从远程车辆接收的验证消息可以包括远程车辆的证书摘要、远程车辆的唯一编号以及远程车辆的唯一编号接收列表。

[0011] 控制器还可以被配置为生成包括主车辆的唯一编号接收列表、主车辆的证书摘要

和主车辆的唯一编号的第二验证消息，以及控制通信单元将生成的第二验证消息发送至远程车辆。

[0012] 控制器还可以被配置为基于从远程车辆接收的包括主车辆的唯一编号的验证消息的次数来确定远程车辆是否可靠。

[0013] 控制器还可以被配置为基于从远程车辆接收的包括主车辆的唯一编号的验证消息的次数来生成信任得分，以及当所计算的信任得分超过阈值得分时确定远程车辆是可靠的。

[0014] 控制器还可以被配置为匹配远程车辆的证书摘要、远程车辆的唯一编号和远程车辆的信任得分，以及将匹配的结果记录在第二验证消息的唯一编号接收列表中。

[0015] 控制器还可以被配置为每秒钟从计算的信任得分减去预定得分。

[0016] 通信单元可以包括：第一通信模块，被配置为从远程车辆接收基本安全消息，并且向远程车辆发送第二基本安全消息；以及第二通信模块，被配置为从远程车辆接收验证消息，并且向远程车辆发送第二验证消息。

[0017] 第二通信模块还可以被配置为基于短程无线通信来发送第二验证消息。

[0018] 第二验证消息的发送距离可以短于第二基本安全消息的发送距离，并且第二验证消息的发送周期可以长于第二基本安全消息的发送周期。

[0019] 此外，根据本公开的实施方式，用于在车辆间通信环境中验证车辆的方法包括：由通信单元从允许参与车辆间通信的远程车辆接收基本安全消息和验证消息；当通信单元在预定时间段内从远程车辆接收到至少预定次数的验证消息时，由控制器确定远程车辆是可靠的；以及由控制器生成许可以利用从远程车辆接收的基本安全消息。

[0020] 从远程车辆接收的验证消息可以包括远程车辆的证书摘要、远程车辆的唯一编号以及远程车辆的唯一编号接收列表。

[0021] 所述确定可以包括由控制器生成包括主车辆的唯一编号接收列表、主车辆的证书摘要以及主车辆的唯一编号的第二验证消息；以及由控制器控制通信单元将所生成的第二验证消息发送到远程车辆。

[0022] 此外，所述确定可以包括由控制器基于从远程车辆接收的包括主车辆的唯一编号的验证消息的次数，确定远程车辆是否可靠。

[0023] 然后，所述确定可以包括由控制器基于从远程车辆接收的包括主车辆的唯一编号的验证消息的次数，生成信任得分；以及当所计算的信任得分超过阈值得分时，由控制器确定远程车辆是可靠的。

[0024] 所述确定可以包括由控制器匹配远程车辆的证书摘要、远程车辆的唯一编号和远程车辆的信任得分；以及由控制器将匹配的结果记录在第二验证消息的唯一编号接收列表中。

[0025] 控制器还可以被配置为由控制器每秒钟从所计算的信任得分减去预定得分。

[0026] 所述方法还可以包括：由通信单元的第一通信模块从远程车辆接收基本安全消息；由第一通信模块向远程车辆发送第二基本安全消息；由通信单元的第二通信模块从远程车辆接收验证消息；以及由第二通信模块向远程车辆发送第二验证消息。

[0027] 第二验证消息可以基于短程无线通信来发送。

[0028] 进一步地，第二验证消息的发送距离可以短于第二基本安全消息的发送距离，并

且第二验证消息的发送周期可以长于第二基本安全消息的发送周期。

附图说明

[0029] 结合附图，从以下详细描述中，本公开的上述和其它目的、特征和优点将变得更加明显：

[0030] 图1是根据本公开的实施方式的车辆间通信环境的示例图；

[0031] 图2是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的装置的示例框图；

[0032] 图3是根据本公开的实施方式的通过用于在车辆间通信环境中验证车辆的装置推导阈值得分计算方程的过程示例图；

[0033] 图4是根据本发明实施方式的用于在车辆间通信环境中验证车辆的装置的测试环境示例图；

[0034] 图5是根据本发明实施方式的在车辆间通信环境中验证车辆的装置的测试结果示例图；以及

[0035] 图6是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的方法的示例流程图。

[0036] 应该理解的是，以上参考的附图不一定按比例绘制，呈现说明本公开的基本原理的各种优选特征的稍微简化的表示。包括例如特定尺寸、取向、位置和形状的本公开的具体设计特征将部分由特定的预期应用和使用环境来确定。

具体实施方式

[0037] 在下文中，将参照附图详细描述本公开的实施方式。在整个说明书中，要注意的是，即使在不同的附图中提供相同或相似的附图标记，也表示相同或相似的部件。此外，在本公开的以下描述中，当可以使得本公开的主题不清楚时，将省略并入本文的已知功能和配置的详细描述。

[0038] 此外，在描述本公开的部件时，可以在本文中使用诸如第一、第二、A、B、(a)、(b)等的术语。这些术语仅用于与其他元素区分的元素，元素的本质、顺序、序列和数量不受这些术语的限制。此外，除非另外定义，否则本文中使用的所有术语(包括技术或科学术语)具有与本公开所属领域的技术人员通常理解的相同含义。在通用字典中定义的术语应该被解释为具有与相关技术的上下文的含义相一致的含义，并且除非在本公开的说明书中清楚地定义，否则不应该被解释为理想的或过于正式的含义。

[0039] 可以理解，在此使用的术语“车辆”或“车辆的”或其它类似的术语包括一般的机动车辆，例如包括运动型多用途车辆(SUV)的客车、公共汽车、卡车、各种商用车辆、包括各种船只和船舶的水运工具、飞机等，并且包括混合动力车辆、电动车辆、插电式混合动力电动车辆、氢动力车辆和其他替代燃料车辆(例如，来自非石油资源的燃料)。如本文所提及的，混合动力车辆是具有两个或更多个动力源的车辆，例如汽油动力和电动动力车辆。

[0040] 另外，可以理解，以下方法或其方面中的一个或多个可以由至少一个控制器执行。术语“控制器”可以指代包括存储器和处理器的硬件设备。存储器被配置为存储程序指令，并且处理器被具体编程为执行程序指令以完成下面进一步描述的一个或多个处理。此外，

可以理解，下面的方法可以由包括控制器的装置与一个或更多个其他部件一起执行，如本领域普通技术人员将理解的那样。

[0041] 现在参考本公开的实施方式，图1是根据本公开的实施方式的车辆间通信环境的示例图，并且将参照主车辆100进行描述。

[0042] 如图1所示，根据本公开的车辆间通信环境(系统)包括主车辆(HV)100和多个远程车辆(RV)200。然后，主车辆100和远程车辆200在同一道路上行驶。

[0043] 主车辆100将包括其车辆信息的基本安全消息(BSM，basic safety message)发送到远程车辆200，远程车辆200将包括其车辆信息的基本安全消息(BSM)发送到主车辆100。然后，远程车辆200的车辆信息是在与主车辆100同一道路上行驶同时位于离主车辆100特定距离内的远程车辆200的行驶信息，并且包括有助于主车辆100安全行驶的信息。

[0044] 为了清楚起见，由远程车辆200发送的基本安全消息在本文中可以被简称为“基本安全消息”(或BSM)，而由主车辆100发送的基本安全消息在本文中可以被称为“第二基本安全消息”(或第二BSM)。类似地，由远程车辆200发送的验证消息在本文中可被简称为“验证消息”，而由主车辆100发送的验证消息在本文中可被称为“第二验证消息”。

[0045] 主车辆100基于从远程车辆200接收的车辆信息来控制安装在主车辆100上的各种安全系统。这里，安全系统包括智能巡航控制(SCC)系统、车道偏离警告系统(LDWS)、侧面障碍警报系统(SOWS)、防撞系统、自动紧急制动(AEB)系统和车道保持辅助系统(LKAS)。

[0046] 同时，位于主车辆100的特定距离内但位于主车辆100行驶道路之外的攻击车辆(AV)300是被允许车辆间通信的车辆。

[0047] 由攻击车辆300发送的车辆信息根本无助于主车辆100的行驶，并且如果恶意用户通过攻击车辆300向车辆100发送虚假信息，则不能保证车辆行驶的安全性。

[0048] 根据本公开，通过以高精度确定攻击车辆100(其提供阻碍主车辆100的安全性的车辆信息)，可以过滤由攻击车辆300发送的消息。

[0049] 根据本公开，主车辆100和远程车辆200可以包括用于支持车辆到任何物体(V2X)无线通信的通信模块，并且车辆通信模块可以支持诸如WCDMA、LET或者Wi-Fi的移动通信，尤其可以通过车载环境(WAVE)无线通信方案中的无线接入来支持与另一车辆、互联网中的服务器、另一个系统或终端的V2X通信。可应用于车辆通信模块的车载环境(WAVE)无线通信协议中的无线接入是IEEE 802.11p标准和IEEE P1609标准的组合，并且是可以通过支持车辆间高速通信和车辆到基础设施的通信而用于构建各种下一代智能交通系统的通信标准之一。WAVE通信方法可以使用路边单元(RSU)的中继，但是也可以直接支持车辆到车辆(V2V)的通信。支持WAVE通信方案的车辆通信模块包括用于支持在200km/h的最大车速下10毫秒或更少的通信延迟、1km的通信半径、54Mbps的最大发送速率、5.850GHz至5.925GHz的使用频率、10MHz的信道带宽和7个信道的物理层和介质访问控制(MAC)层，并且可以确保高速移动性。

[0050] 在本公开的V2X通信环境中，根据必要信号的产生，车辆通信模块可以与RSU或服务器进行通信，以通过用户(诸如驾驶员)的操纵或者另一种方法来发送和接收必要的信息。另外，车辆通信模块可以连接到由用户使用的诸如移动通信终端(例如，智能电话、PDA和PDA)或安装在车辆上的导航终端的各种人机界面(HMI)电子设备，并且可以根据必要信号的产生与RSU或服务器通信，以通过由诸如驾驶员的用户的HMI的操纵或其他方法来发送

和接收必要的信息。车辆通信模块可以包括用户界面，并且可以根据用户请求与RSU或服务器进行通信，以发送和接收信息。

[0051] 图2是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的装置的示例框图，并且车辆验证装置可以安装到被允许车辆间通信的所有车辆，并且将参考安装在主车辆100上的车辆验证装置。另外，假设主车辆100通过认证对所有远程车辆200和攻击车辆300允许车辆间通信。

[0052] 如图2所示，根据本公开的用于在车辆间通信环境中验证车辆的装置包括通信单元10、控制器20和存储器30。

[0053] 在元件的描述中，通信单元10可以包括第一通信模块11和第二通信模块12，第一通信模块11被配置为发送基本安全消息(BSM)到远程车辆200和从远程车辆200接收基本安全消息(BSM)，第二通信模块12被配置为发送验证消息到远程车辆200和从远程车辆200接收验证消息。

[0054] 这里，基本安全消息指的是包括车辆信息的消息，验证消息指的是包括验证信息(证书摘要、唯一编号和自然列表接收列表)的消息。然后，证书摘要是一种数据格式，并且可以通过32字节的散列值来实现，并且唯一编号接收列表指的是其中记录了发送验证消息的车辆(终端)的唯一编号的列表。

[0055] 第一通信模块11基于作为一种专用短程通信(DSRC)技术的车载环境(WAVE)通信方案中的无线接入来发送和接收基本安全消息。作为实例，第一通信模块11可以23dBm的发送功率和10Hz的发送周期(每秒10次)发送基本安全消息(即，第二基本安全消息)。

[0056] 第二通信模块12基于短程通信方案发送验证消息到远程车辆200和从远程车辆200接收验证消息。第二通信模块可以通过使用蓝牙TM、射频识别(RFID)、红外数据组织(IrDA)、超宽带(UWB)、ZigBee、近场通信(NFC)、无线保真(Wi-Fi)、Wi-Fi直连、无线通用串行总线(USB)技术中的至少一个来支持短程通信。作为示例，第二通信模块12可以9dBm的发送功率(低功率)和7Hz(每一秒7次)的发送周期发送第二验证消息。第二验证消息的发送距离比第二基本安全消息的发送距离短。

[0057] 接下来，控制器20执行整体控制，使得元件可以正常执行其功能。

[0058] 此外，控制器20可以在车辆间通信环境中通过使用基于短程无线通信的验证消息来验证远程车辆，来确定被允许车辆间通信的远程车辆所发送的信息是否可信。也就是说，控制器20将位于第二通信模块12的通信区域中达特定时间段的远程车辆200确定为可信车辆，并且相应地，将由可信远程车辆200发送的基本安全消息确定为可信的基本安全信息。

[0059] 此外，控制器20可以允许由可信远程车辆200发送的基本安全消息(车辆信息)被用在各种系统中。

[0060] 在下文中，将详细描述由控制器20验证远程车辆200的过程。

[0061] 1)控制器20发送验证消息(即，第二验证消息)到远程车辆200的过程：

[0062] 控制器20通过通信单元10中的第二通信模块12从远程车辆200接收验证消息，并将包含在接收的验证消息中的远程车辆200的唯一编号记录在唯一编号接收列表中。然后，主车辆100的唯一编号接收列表被存储在存储器30中。此外，当远程车辆200位于主车辆100的第二通信模块12的通信区域中时，主车辆100周期性地从远程车辆200接收验证消息。

[0063] 此后，控制器20生成包括主车辆100的证书摘要、主车辆100的唯一编号以及主车

辆100的唯一编号接收列表的第二验证消息，并发送该验证消息到远程车辆200。然后，当远程车辆200位于主车辆100的第二通信模块12的通信区域中时，主车辆100周期性地发送第二验证消息到远程车辆200。

[0064] 2)由控制器20管理远程车辆200的信任得分的过程：

[0065] 控制器20通过通信单元10中的第二通信模块12从远程车辆200接收验证消息，并且识别主车辆100的唯一编号是否包含在所接收的验证消息中所包含的远程车辆的唯一编号接收列表中。这是识别主车辆100之前是否已经向远程车辆200发送了验证消息的过程。

[0066] 此后，如果主车辆100的唯一编号包含在远程车辆200的唯一编号接收列表中，则控制器20将一个得分添加到用于确定远程车辆200的可信度的信任得分。

[0067] 此后，控制器20在验证消息接收列表中记录远程车辆200的证书摘要、远程车辆200的唯一编号以及远程车辆200的信任得分。

[0068] 此后，控制器20确定在验证消息接收列表上远程车辆200的累积的信任得分是否超过预定义的阈值得分，并且如果累积的信任得分超过预定义的阈值得分，则确定远程车辆200是可信的。

[0069] 同时，控制器20周期性地(例如，以一秒为单位)从远程车辆200的信任得分减去一个得分。如果远程车辆200的信任得分没有被连续添加，那么甚至不信任曾经被信任的远程车辆200。

[0070] 在下文中，将参照图3详细描述计算阈值得分的过程。

[0071] 图3是根据本公开的实施方式的通过用于在车辆间通信环境中验证车辆的装置导出阈值得分计算方程的过程示例图。

[0072] 如图3所示，ⓐ、ⓑ、ⓒ和ⓓ四个区域指示主车辆100可以从攻击车辆300接收基本安全消息的区域。用于确定攻击车辆300在每个区段中是否可信的参考遵照是否唯一的主车辆100的编号被记录在攻击车辆300的唯一编号接收列表中。

[0073] 在区域ⓐ中，主车辆100位于距远程车辆A 201的特定距离dw内，并且类似地，远程车辆A 201位于距攻击车辆300的特定距离dw内。此外，攻击车辆300距主车辆100比特定距离dw更远，但是比2倍特定距离2×dw更近。

[0074] 远程车辆A 201接收主车辆100的验证消息(即，第二验证消息)，并且将包含在主车辆100的验证消息中的主车辆100的唯一编号记录在远程车辆A 201的唯一编号接收列表中。

[0075] 攻击车辆300可以接收远程车辆A 201的验证消息，并且可以将远程车辆A 201的唯一编号接收列表上的主车辆100的唯一编号和包含在远程车辆A 201的验证消息中的远程车辆A 201的唯一编号记录在攻击车辆300的唯一编号接收列表中。因此，尽管攻击车辆300实际上并未从主车辆100接收到验证消息，攻击车辆300可以通过远程车辆A 201获取主车辆100的唯一编号。

[0076] 如果攻击车辆300通过改变发射功率将攻击车辆300的验证消息发送到主车辆100，则主车辆100确定攻击车辆300是可信的，因为主车辆100的唯一编号被记录在攻击车辆300的验证消息中的唯一编号接收列表中。

[0077] 因为主车辆100确定攻击车辆300是可信的车辆，所以主车辆100可能从攻击车辆

300接收包含无意义信息或虚假信息的基本安全消息。

[0078] 此后,如果主车辆100行驶并进入区域ⓑ,则主车辆100位于距攻击车辆300的特定距离dw内。因为当主车辆100在区域ⓑ中移动时攻击车辆300可以接收主车辆100的验证消息,所以攻击车辆300可以将主车辆100的唯一编号记录在攻击车辆300的唯一编号接收列表中。

[0079] 如果攻击车辆300发送其自己的验证消息,则接收到该验证消息的主车辆100确定攻击车辆300是可信的,因为主车辆100的唯一编号被记录在攻击车辆300的唯一编号接收列表中。

[0080] 因为主车辆100确定攻击车辆300是可信的车辆,所以主车辆100可能从攻击车辆300接收包含无意义信息或虚假信息的基本安全消息。

[0081] 在区域ⓒ中,主车辆100位于距离远程车辆B 202的特定距离dw内,并且远程车辆B 202位于距离攻击车辆300的特定距离dw内。此外,攻击车辆300距主车辆100比特定距离dw更远,但比2倍特定距离2×dw更近。

[0082] 远程车辆B 202接收主车辆100的验证消息,并且将包含在主车辆100的验证消息中的主车辆100的唯一编号记录在远程车辆B 202的唯一编号接收列表中。

[0083] 攻击车辆300可以接收远程车辆B 202的验证消息,并且可以将远程车辆B 202的唯一编号接收列表上的主车辆100的唯一编号和包括在远程车辆B 201的验证消息中的远程车辆B 202的唯一编号记录在攻击车辆300的唯一编号接收列表中。因此,尽管攻击车辆300实际上并没有从主车辆100接收到验证消息,攻击车辆300可以通过远程车辆B 202获取主车辆100的唯一编号。

[0084] 如果攻击车辆300通过改变发射功率将攻击车辆300的验证消息发送到主车辆100,则主车辆100确定攻击车辆300是可信的,因为主车辆100的唯一编号在攻击车辆300的唯一编号接收列表中。

[0085] 因为主车辆100确定攻击车辆300是可信的车辆,所以主车辆100可能从攻击车辆300接收包含无意义信息或虚假信息的基本安全消息。

[0086] 区域ⓓ表示考虑到主车辆100的速度和消息更新时间周期,即使当主车辆100与攻击车辆300分开超过两倍特定距离(2×dw)的距离时也可以接收到基本安全消息的区域。

[0087] 当主车辆100移动到点V'时,主车辆100的唯一编号留在攻击车辆300的唯一编号接收列表中。然后,V'表示通过将主车辆100的速度v乘以唯一编号的交换时段t_{up}获得的结果(距离)。

[0088] 如果攻击车辆300通过改变发射功率将攻击车辆300的验证消息发送到主车辆100,则主车辆100确定攻击车辆300是可信的,因为主车辆100的唯一编号处于攻击车辆300的唯一编号接收列表。

[0089] 当主车辆100移动到点V'时,主车辆100可能从攻击车辆300接收包含无意义信息或虚假信息的基本安全消息。

[0090] 这里,当攻击车辆300的验证消息的发送频率是c Hz时,攻击车辆300的验证消息甚至可以在1/c秒之后到达。

[0091] 因此,在主车辆100以速度v移动到点V'时,主车辆100可以从车辆300接收基本安

全消息的距离$d(t_{up})$可以在下面的等式1中表示。

[0092] [等式1]

[0093] $d(t_{up})=v\times(t_{up}+1/c)$

[0094] 这里,在等式1中,v表示主车辆100的速度,t_{up}表示唯一编号的交换时段(时间段),以及c表示攻击车辆300的验证消息发送频率。

[0095] 结果,主车辆100可以从攻击车辆300接收基本安全消息的最大距离dx可以如以下等式2中所示。

[0096] [等式2]

[0097] $dx=4\times dw+v\times(t_{up}+1/c)$

[0098] 这里,在等式2中,dw表示区域的距离(即,验证消息的发送距离)。

[0099] 同时,当验证消息的发送周期为fw Hz时,由于攻击车辆300的信任得分每秒被减去一个得分,因此可以在一秒获得最大得分(fw-1)。另外,当主车辆100以速度v移动时所耗费的时间段为dx/v。

[0100] 因此,阈值得分θH可以表示成可由主辆100在一秒内在区域Dx中获得的远程车辆200的最大得分与主车辆100移动区域dx所用的时间段的乘积。这如下面的等式3所示。

[0101] [等式3]

[0102] $\theta H=(fw-1)\times dx/v$

[0103] 接下来,存储器30存储验证消息接收列表,在验证消息接收列表中匹配并记录从远程车辆200接收的验证消息中包括的远程车辆200的证书摘要和远程车辆200的唯一编号以及由控制器20计算出的远程车辆200的信任得分。

[0104] 此外,存储器30还可以存储唯一编号接收列表,在唯一编号接收列表中记录从远程车辆200接收的验证消息中包括的远程车辆200的唯一编号。

[0105] 存储器30可以包括闪存类型、硬盘类型、固态硬盘(SSD)类型、硅盘驱动器(SDD)类型、多媒体卡微型类型的至少一种类型的存储介质,或者卡型存储器(例如SD或XD存储器)、随机存取存储器(RAM)、静态随机存取存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROm)、磁存储器、磁盘和光盘。

[0106] 图4是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的装置的测试环境的示例图。

[0107] 如图4所示,测试是在四车道公路上进行的,具体情况如下。

[0108] 公路车道宽度为3m,车辆之间的间距为33.3m,车速为120km/h,由攻击车辆300发送的基本安全信息的发送功率为23dBm,由攻击车辆300发送的基本安全消息的发送周期为10Hz,由攻击车辆300发送的验证消息的发送功率为9dBm,由攻击车辆300发送的验证消息的发送周期为7Hz。

[0109] 在攻击车辆300停止并且调整攻击车辆300和公路之间的距离dk时,观察在应用本公开的公路上的车辆是否利用了由受控的攻击车辆300发送的基本安全消息。然后,当公路上的特定车辆利用由攻击车辆300发送的基本安全消息时,称为攻击成功。例如,基本安全消息是报告车辆在K'点停车的虚假信息。

[0110] 结果如图5所示。

[0111] 图5是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的装置的测试

结果的示例图。

[0112] 如图5所示，纵轴表示每一秒的攻击成功次数，横轴表示攻击车辆300与公路之间的距离。然后，攻击成功次数指的是利用由受控的攻击车辆300发送的基本安全消息的车辆数。

[0113] 附图标记410表示未应用本公开时的成功次数，附图标记420表示当应用本公开时的成功次数。

[0114] 当不应用本公开时(410)，可以看出大多数车辆利用由受控的攻击车辆300发送的基本安全消息。然后，利用由受控的攻击车辆300发送的基本安全消息的车辆数在大约460m处减少的原因是：由基本安全消息的发送距离引起的，并且能够看出，公路上的车辆不能接收到由攻击车辆300发送的基本安全消息，因为如果攻击车辆300与公路相距约710m，则其完全脱离了攻击车辆300的通信距离。

[0115] 同时，当应用本公开时(420)，能够看出，不管距离如何，公路上的车辆都不利用由受控的攻击车辆300发送的基本安全消息。

[0116] 图6是根据本公开的实施方式的用于在车辆间通信环境中验证车辆的方法的示例流程图。

[0117] 首先，通信单元10发送基本安全消息和验证消息到被允许车辆间通信的远程车辆，以及从被允许车辆间通信的远程车辆接收基本安全消息和验证消息(601)

[0118] 此后，当验证消息在预定时间段内被接收预定次数时，控制器20确定远程车辆是可信的，以允许利用远程车辆发送的基本安全消息(602)。

[0119] 根据本公开的实施方式，可以通过使用基于在车间环境中的短程无线通信的验证消息验证远程车辆，确定由被允许车辆间通信的远程车辆发送的信息是否可信。

[0120] 以上描述是本公开的技术精神的简单示例，并且本公开内容可以由本公开所属领域的技术人员进行各种修改和修改，而不偏离本公开的基本特征。

[0121] 因此，本发明的公开实施方式不限制本发明的技术精神，而是示例性的，而且本发明的技术精神的范围不受本发明实施方式的限制。本公开的范围应该由权利要求来解释，并且将理解的是，在等同范围内的所有技术精神落入本公开的范围内。

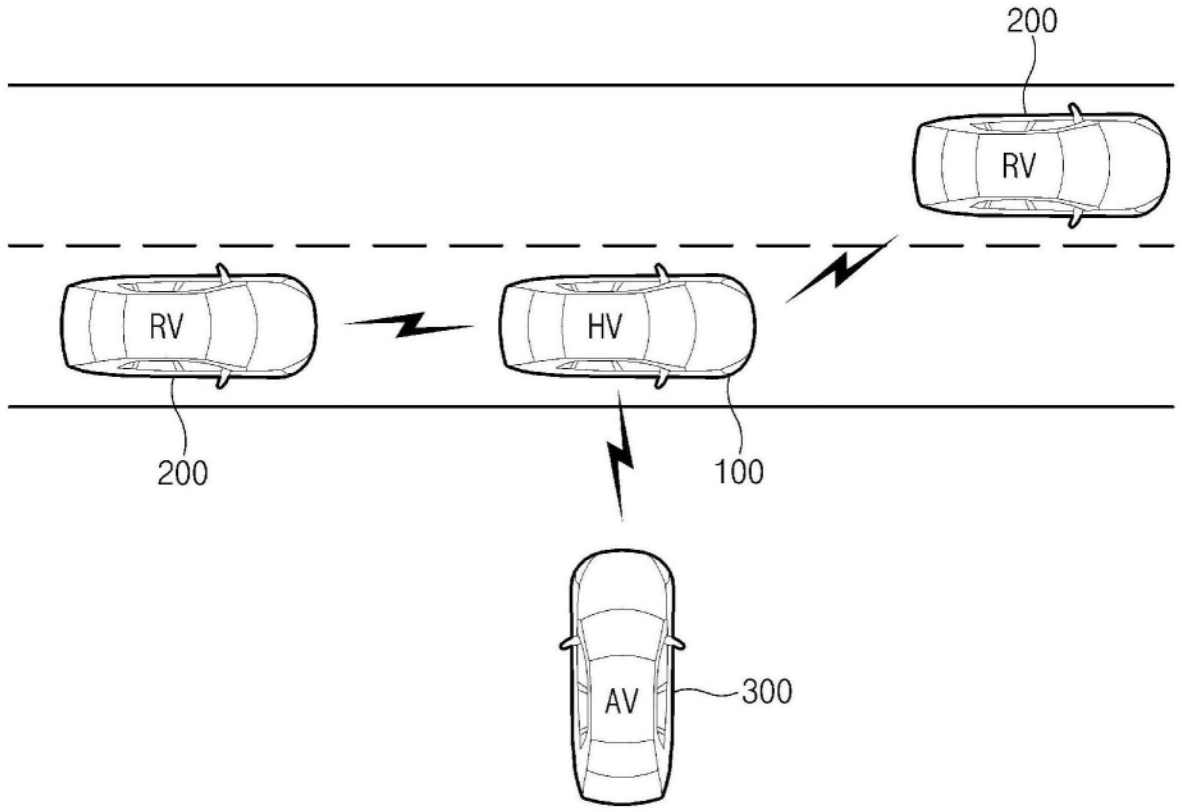

200
RV
RV
HV
200
100
AV
300

图1

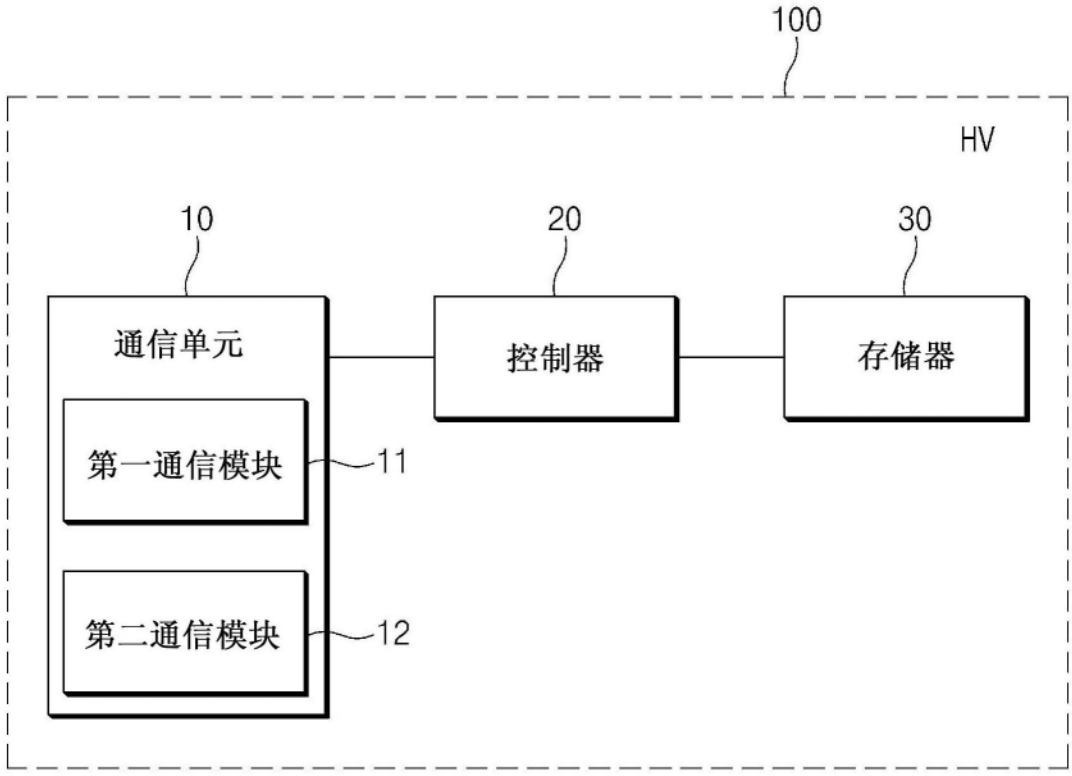

100
HV
10
20
30
通信单元
控制器
存储器
第一通信模块
11
第二通信模块
12

图2

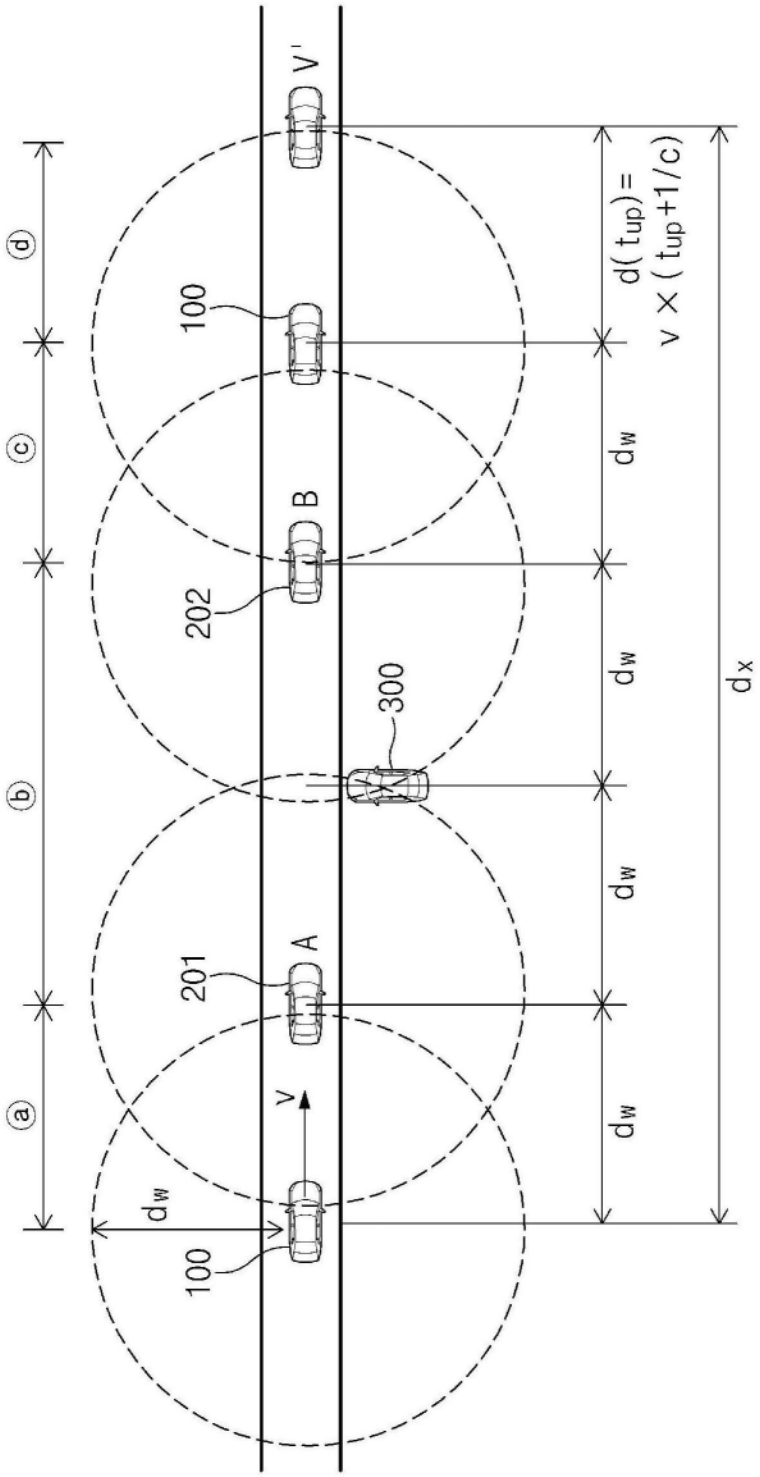


图3

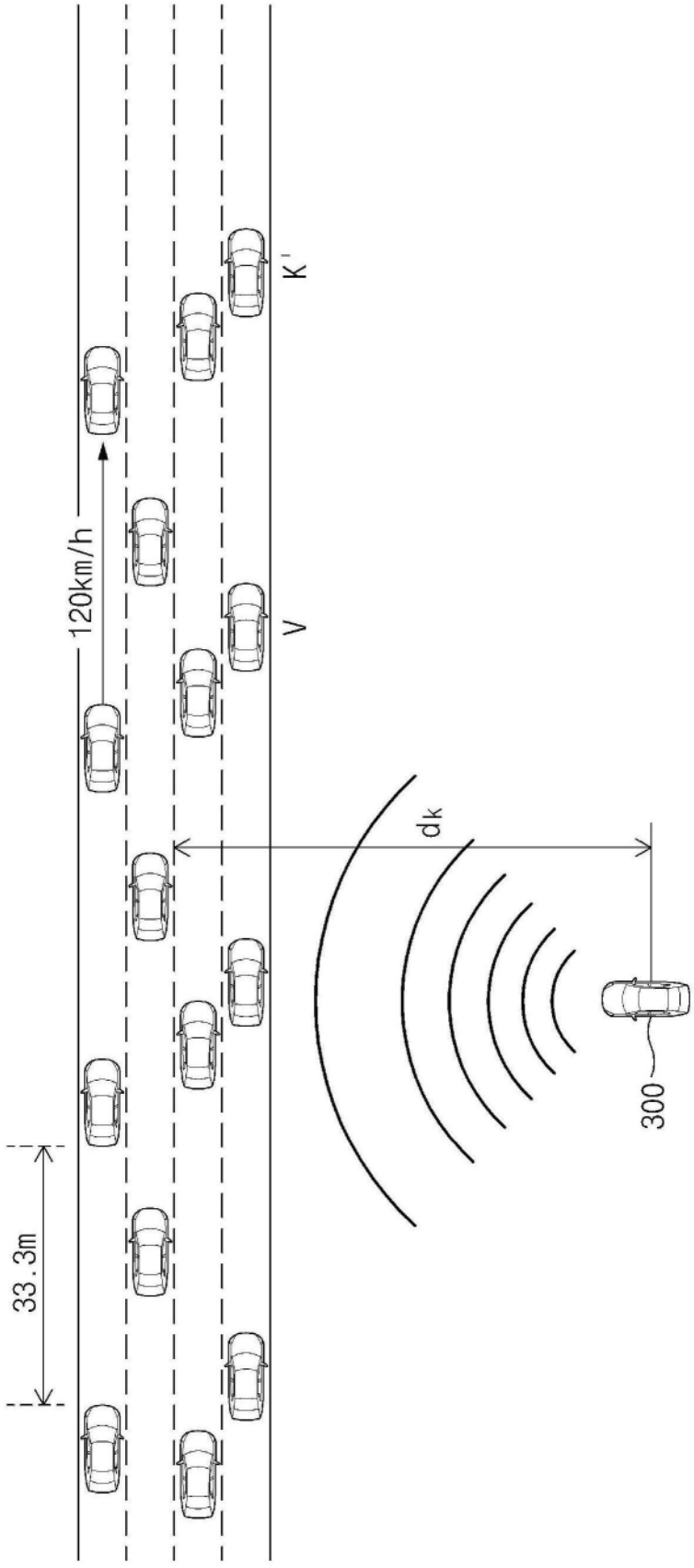


图4

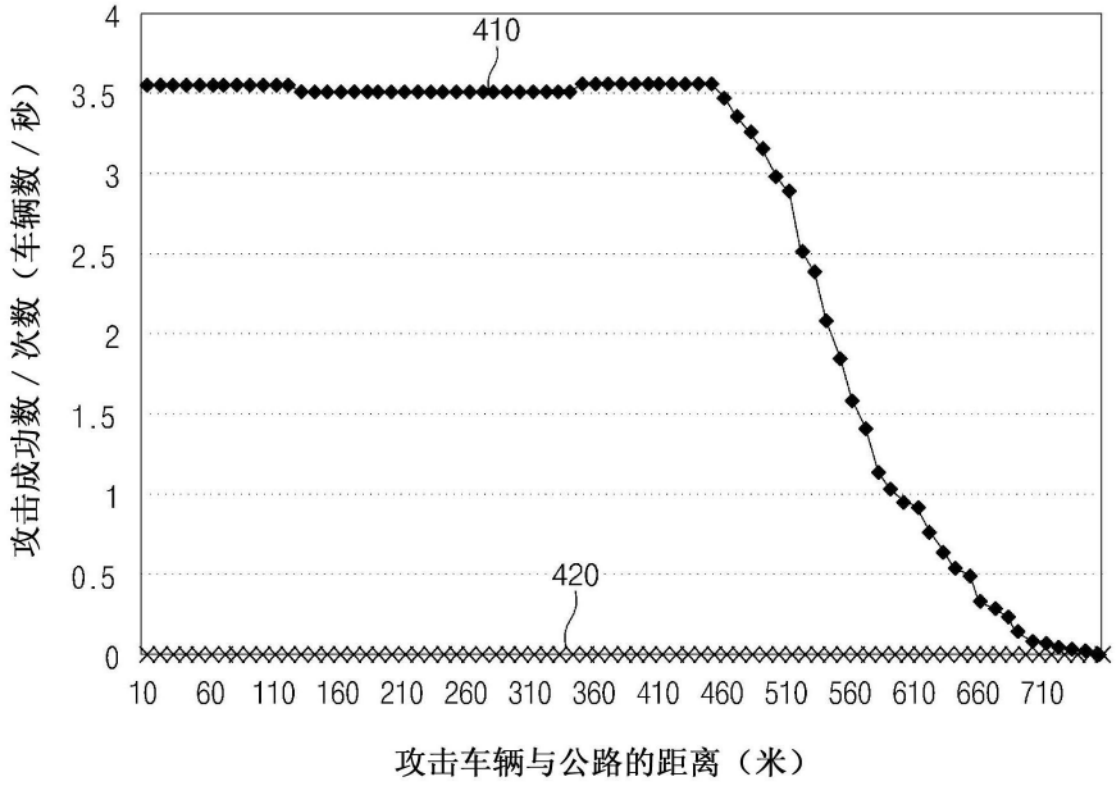

410
420
攻击成功数 / 次数（车辆数 / 秒）
4
3.5
3
2.5
2
1.5
1
0.5
0
10 60 110 160 210 260 310 360 410 460 510 560 610 660 710
攻击车辆与公路的距离（米）

图5

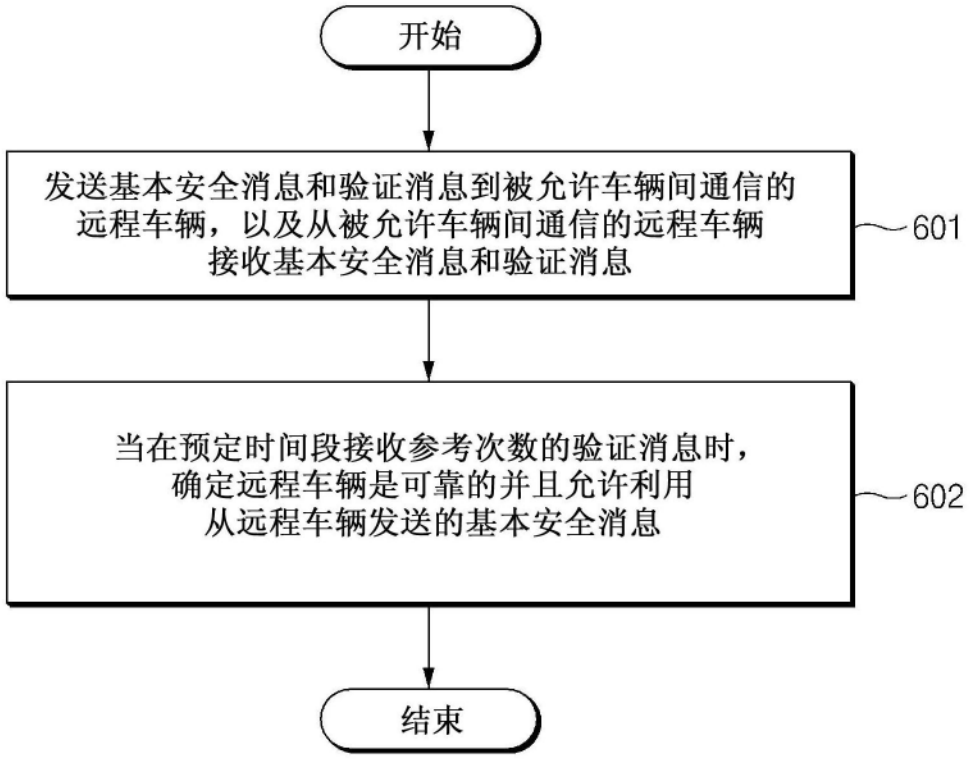

开始
发送基本安全消息和验证消息到被允许车辆间通信的远程车辆，以及从被允许车辆间通信的远程车辆接收基本安全消息和验证消息
601
当在预定时间段接收参考次数的验证消息时，确定远程车辆是可靠的并且允许利用从远程车辆发送的基本安全消息
602
结束

图6