(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 3 月 5 日 (05.03.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/042844 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2019/098056

(22) 国际申请日: 2019 年 7 月 27 日 (27.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810976472.9 2018年8月25日 (25.08.2018) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

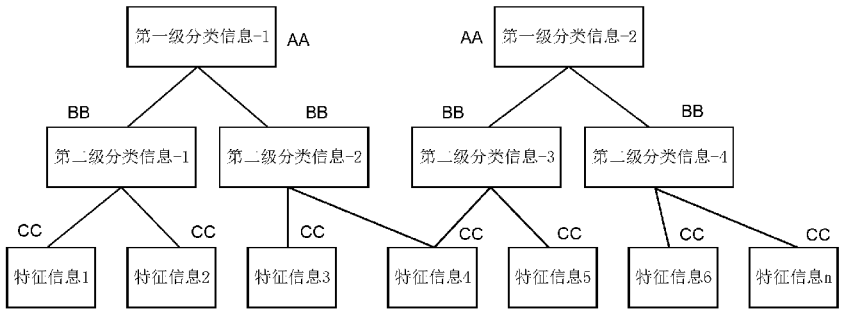
(72) 发明人: 李飞(**LI, Fei**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 朱锦涛(**ZHU, Jintao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 何承东(**HE, Chengdong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 白涛(**BAI, Tao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,

(54) **Title:** METHOD FOR DETERMINING CERTIFICATE STATE

(54) 发明名称: 确定证书状态的方法



AA FIRST-LEVEL CLASSIFICATION INFORMATION
BB SECOND-LEVEL CLASSIFICATION INFORMATION
CC FEATURE INFORMATION

图 3

(57) **Abstract:** The present application, in order to satisfy real-time and security requirements of Internet of Vehicles communications, provides a method enabling an information receiving end to quickly determine a certificate state. In the invention, classification information of a certificate is comprised in an agreement field of the certificate, and classification information of a revoked certificate is comprised in an agreement field of a certificate revocation list, such that a receiving end can, according to classification information in a certificate of a sending end, quickly narrow a search or match range when searching a large number of records of the certification revocation list, thereby improving speed and efficiency in determining a certificate state.

(57) 摘要: 为满足车联网通信中实时性和安全性的需求，本申请提出一种能够使消息接收端快速确认证书状态的方法。通过在证书的约定字段中包含证书的分类信息，并在证书吊销列表的约定字段中包含被吊销证书的分类信息，接收端能够根据发送端证书中携带的分类信息，在证书吊销列表海量的记录中快速缩小搜索或匹配的范围，以提高确定证书状态的速度和效率。

WO 2020/042844 A1

[见续页]

IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

确定证书状态的方法

本申请要求于 2018 年 8 月 25 日提交中国国家知识产权局、申请号为 201810976472.9、申请名称为“确定证书状态的方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，尤其涉及车联网领域设备间通信时，确定证书的状态的方法、装置和系统。

背景技术

V2X（Vehicle to Everything）车联网指的是车辆之间，或者车辆与行人或骑行者之间以及车辆与基础设施之间的通信系统。车联网通信具有消息量大且消息收发频率高的特点，如车载通信单元（on-board unit, OBU）或路侧通信单元（road side unit, RSU）周期性（如 10 赫兹）发送描述车辆运行状态（速度、朝向、方位）的协作感知消息（cooperative awareness message, CAM），或当发生特殊事件时，发送描述事件类型的分散环境通知信息（Decentralized Environmental Notification Message, DENM）。

出于安全性考虑，通信系统中通常使用证书进行数据源认证，如发送端在发送的消息中携带证书，接收端对消息中携带的证书进行验证，其中包括验证证书是否已被吊销。在传统互联网通信领域使用 OCSP 方案，即客户端使用在线证书状态协议（Online Certificate Status Protocol, OCSP）到 OCSP 服务器实时查询证书是否被吊销。

在车联网通信中，同样需要使用证书进行数据源认证，但传统的 OCSP 方案并不适用于车联网通信的场景。以 CAM 消息为例，车辆每秒广播 10 条 CAM 消息，理论上以车辆为中心半径 1 千米内的全部车辆都会受到广播的 CAM 消息，如果采用 OCSP 方案，每辆接收到 CAM 消息的车辆都需要对每条 CAM 消息中的证书进行实时查询，不仅会对 OCSP 服务器的性能和网络带宽造成巨大负担，而且车辆与 OCSP 服务器间的通信，会额外增加车联网通信的时延。

因此，为满足车联网通信中实时性和安全性的需求，亟需一种效率更高的判断证书是否被吊销的方法。

发明内容

为满足车联网通信中实时性和安全性的需求，本申请提出一种能够使消息接收端快速确认证书状态的方法。本申请中所述的证书状态指证书是否被吊销。

本申请实施例提出一种基于证书吊销列表的方案，该方案中提出证书的分类信息和证书的特征信息两个概念。证书的分类信息指为证书颁发服务器在颁发证书时为证书分配的一个类别信息，用于对证书进行分类。证书的特征信息指可以唯一识别一个证书的信息，证书的特征信息可以是证书颁发服务器在颁发证书时为证书分配的一个 n 个字节的随机数，还可以是对该证书进行哈希计算后截取的 n 个字节的数值。

本申请实施例提出在证书的约定字段中包含证书的分类信息，并在证书吊销列表的约定字段中包含被吊销证书的分类信息。另外，当证书的特征信息为证书颁发服务器在颁发证书时为证书分配的一个 n 个字节的随机数时，一种可能的实现方式中，证书的特征信息可以包

含在证书的某一约定字段。证书吊销列表中除了记录被吊销证书的分类信息，还需要在某一约定字段包含被吊销证书的特征信息。

证书吊销列表由证书吊销服务器生成并维护。车联网中的通信单元，如接收端和发送端，从证书吊销服务器获取证书吊销列表。接收端在接收到消息后，根据保存的证书吊销列表，对消息发送端证书进行验证，确定证书的状态。通过在证书的约定字段中包含证书的分类信息，并在证书吊销列表的约定字段中包含被吊销证书的分类信息，接收端能够根据发送端证书中携带的分类信息，在证书吊销列表海量的记录中快速缩小搜索或匹配的范围，以提高证书验证的速度和效率。具体的，接收端在证书吊销列表中，确定与发送端证书具有相同分类信息的被吊销证书的记录集合，并进而在该集合中确定与发送端证书具有相同特征信息的被吊销证书的记录，如果存在匹配的记录，则发送端证书已被吊销，如果不存在匹配的记录，则发送端证书未被吊销。

另外，本申请实施例还提出一种基于证书吊销指纹库的方案。证书吊销服务器将被吊销证书的指纹信息录入证书吊销指纹库。车联网中的通信单元，如接收端和发送端，从证书吊销服务器获取证书吊销指纹库。接收端在接收到消息后，提取消息发送端证书的指纹信息，根据保存的证书吊销指纹库，对消息发送端证书进行验证，确定证书的状态。为提高通信效率，本申请实施例提出证书吊销服务器维护一个证书吊销指纹位置库，以保存一段时间内证书吊销指纹库中记录的变化情况，车联网通信单元获取证书吊销指纹位置库，就可以刷新保存的证书吊销指纹库。为了提高证书吊销指纹库方案的准确性，本申请实施例还提出发送端自验证书是否被吊销的方案，确保消息中携带的证书为证书吊销指纹库中无匹配记录的证书，以防止接收端误判。

为配合本申请权利要求部分所述的方法，接收端也需要进行相应的改进，以支持本申请实施例中所述的确定证书状态的方法。

证书吊销列表方案中，发送端向接收端发送的消息中包括发送端的证书，由于发送端的证书中包括分类信息，接收端可以根据发送端证书的分类信息，与证书吊销列表中被吊销证书的分类信息进行匹配，并根据匹配结果确定所述发送端的证书的状态。

证书吊销指纹库方案中，发送端根据保存的证书吊销指纹库，在发送端的证书中确定一个证书吊销指纹库中没有匹配记录的证书，并在发送的消息中使用该选定的证书。

一种可能的实现方式中，发送端计算获得发送端任一证书的指纹信息，如果发送端判断证书吊销指纹库中不存在与该证书的指纹信息匹配的指纹信息，则在发送的消息中使用该证书。

另一种可能的实现方式中，发送端计算获得发送端任一证书的指纹信息，如果发送端判断证书吊销指纹库中存在与该证书的指纹信息匹配的指纹信息，则选择与该证书不同的第二证书，并继续计算第二证书的指纹信息，并判断证书吊销指纹库中是否存在与第二证书的指纹信息匹配的指纹信息。

本申请实施例中所述的方法涉及接收端、发送端、证书吊销服务器和车联网服务器等装置。因此，本申请实施例还提供实现如上证书验证方法的装置和服务器。

另外，本申请实施例还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，当其在计算机上运行时，使得计算机执行上述证书验证方法。

最后，本申请提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述证书验证方法。

附图说明

图 1 所示为本申请实施例提供的一种车联网系统架构图；

图 2 所示为本申请实施例提供的一种车联网通信方法流程图；

图 3 所示为本申请实施例提供的一种将证书进行分级分类的结构示意图；

图 4 所示为本申请实施例提供的一种吊销证书的方法流程图；

图 5 所示为本申请实施例提供的一种从证书吊销服务器获取被吊销证书信息的方法流程图；

图 6 所示为一种证书吊销指纹库的数据结构示意图；

图 7 所示为本申请实施例提供的一种自验证书的车联网通信方法流程图；

图 8 所示为本申请实施例提供的一种确认证书状态的方法流程图；

图 9 所示为本申请实施例中所述装置采用的装置结构示意图。

具体实施方式

为满足车联网通信中实时性和安全性的需求，本申请实施例提出一种相比现有技术，效率更高的判断证书是否被吊销的方法。需要说明的是，本申请实施例中所述的证书，指通信领域中使用的数字证书。

图 1 所示为本申请实施例提出的一种车联网系统架构，其中包括证书颁发服务器，证书吊销服务器，车联网服务器和车联网终端。其中车联网终端也可以是车联网装置或设备，如车载通信单元或路侧通信单元或行人所携带的通信装置。车联网终端从证书颁发服务器获取证书，直接或间接从证书吊销服务器获取证书吊销列表(Certificate Revocation List，CRL)。CRL 为证书吊销服务器生成的，用于记录已被吊销证书的信息。车联网终端向车联网服务器上报车联网终端的状态，运行信息和异常信息。车联网服务器可以直接向证书吊销服务器请求吊销某一车联网终端的证书，也可以通过证书颁发服务器向向证书吊销服务器请求吊销某一车联网终端的证书。

图 2 所示为本申请实施例提出的一种车联网通信业务流程示意图。通信流程涉及两个车联网终端、装置或设备，根据通信角色的不同，分为发送端和接收端。

发送端在 101 步骤发送的消息中携带发送端的证书。发送端发送的证书中包含分类信息。分类信息为证书颁发服务器在颁发证书时为证书分配的一个类别信息，用于对证书进行分类；分类的维度本申请不进行限定，可以以地理方位为维度，如将证书颁发服务器所在的地理方位作为分类信息，也可以以行政区域为维度，如将证书颁发服务器所在的行政区域作为分类信息。分类信息的格式和长度，本申请也不进行限定，分类信息可以是包含多个级别的多级分类信息，也可以是一级分类信息。分类信息可以通过多种方式携带，本申请实施例以 IEEE 1609.2 标准定义的车联网证书格式为例，列举几种可能的证书中携带分类信息的方式。

```
IEEE1609.2 CertificateBase {
        ……
        toBeSigned {
                id,
                cracaId,
                crlSeries,
                region,
                ……}
```

```
        ……,
}
```

第一种方式：通过 id 证书标识字段携带分类信息。以二级分类信息为例。id 的格式定义为“第一级分类信息|第二级分类信息|特征信息”，其中“|”为连接运算符。当采用证书颁发服务器的行政区域作为分类信息时，第一级分类信息可以是证书颁发服务器所在的省级信息，第二级分类信息可以是证书颁发服务器所在的地市信息。在第一种方式中，特征信息为为证书颁发服务器在生成证书时为证书分配的用于标识该证书的信息，特征信息可以记录在证书的任一约定字段中。一种可能的实现方式中，特征信息可以是使用随机数生成器生成的 n 个字节的二进制数字。第一种方式中，两个不同分类信息的证书，其特征信息可以相同。假设第一级分类信息长度为 1 个字节，第二级分类信息长度为 1 个字节，n 为 1，则一个可能的证书的 id 的取值为“100010000001000111111110”，其中“10001000”为证书的第一级分类信息，“00010001”为第二级分类信息，“11111110”为随机数。

第二种方式：通过 region 区域字段携带分类信息。Region 的格式定义为“第一级分类信息|第二级分类信息”。

第三种方式：通过 crlSeries 证书吊销系列字段携带分类信息，或通过 cracaId 证书吊销服务器标识和 crlSeries 字段携带分类信息。如 crlSeries 字段的格式定义为“第一级分类信息|第二级分类信息”；或通过 cracaId 字段携带第一级分类信息，通过 crlSeries 字段携带第二级分类信息。如 cracaId 字段记录负责对该证书进行吊销的证书吊销服务器的标识，以此作为第一级分类信息；crlSeries 字段记录该证书一旦被吊销，所归属的 CRL 系列，以此作为第二级分类信息。

接收端在处理消息之前，在 102 步骤首先根据本地保存的证书吊销列表 CRL，验证证书是否被吊销，如果证书已被吊销，则直接丢弃消息。接收端在验证证书之前，直接或间接从证书吊销服务器获取 CRL。与证书中包含的分类信息相对应，接收端本地保存的 CRL 中也需要记录被吊销证书的分类信息。此外，CRL 中还需要记录被吊销证书的特征信息。CRL 中记录被吊销证书的分类信息的字段可以是任意字段，本申请中为描述方便，统一将记录被吊销证书的分类信息的字段称之为吊销标识，吊销标识用于在 CRL 中唯一标识一个被吊销的证书。如下为 IEEE 1609.2 标准定义的 CRL 格式，假设承担吊销标识功能的字段为 CRL 中的 id 字段。同时，假设 id 字段记录被吊销证书的特征信息。当然，还可以选用不同于吊销标识字段的其它字段记录被吊销证书的特征信息。

```
CrlContents ::= SEQUENCE {
        ……
        typeSpecific CHOICE {
                ……
                        entries SequenceOfHashBasedRevocationInfo{
                            id,
                            ……,
                        }
                    }
                ……,
        }
}
```

以二级分类信息为例。CRL 中 id 字段的格式定义为“第一级分类信息|第二级分类信息|被吊销证书的特征信息”，其中“|”为连接运算符，任一证书的特征信息可以是 n 个字节的随机数，还可以是对该证书进行哈希计算后截取的 n 个字节的数值，证书的特征信息用于唯一标识一个证书。当被吊销证书的特征信息为 n 个字节的随机数时，这 n 个字节的随机数可以是从被吊销证书中约定字段提取的信息，如与证书中包含分类信息的第一种方式相对应，截取被吊销证书标识中的 n 个字节的随机数。第一级分类信息可以是被吊销证书的证书颁发服务器所在的省级信息，第二级分类信息可以是被吊销证书的证书颁发服务器所在的地市信息。假设第一级分类信息长度为 1 个字节，第二级分类信息长度为 1 个字节，n 为 1，则一个可能的 CRL 中的 id 的取值为“100010000001000111111110”，其中“10001000”为被吊销证书的的第一级分类信息，“00010001”为第二级分类信息，“11111110”为被吊销证书标识中截取的随机数。

基于如上的定义，接收端在图 2 中第 102 步验证证书的时候，就可以使用接收到的证书中包含的分类信息和提取的接收到的证书的特征信息，快速高效地与 CRL 中吊销标识进行匹配，以确定发送端的证书是否被吊销。如图 3 所示，CRL 列表中记录的吊销标识可以根据分类信息归类在不同的集合和子集合中。假设接收端收到的证书中携带的 id 取值为“100010000001000111111110”；接收端本地保存的 CRL 中，吊销标识的第一级分类信息可以分为两大类，即第一级分类信息-1 和第一级分类信息-2，其中第一级分类信息-1 取值为“10001000”，则接收端验证证书是否被吊销时，只需要匹配查找第一级分类信息为第一级分类信息-1 的吊销标识；然后，接收端根据接收到的证书中 id 包含的第二级分类信息“00010001”，继续缩小匹配查找的范围，第一级分类信息为“00010001”的吊销标识；当存在多级分类信息时，类似的，接收端根据不同级别的分类信息，逐级缩小需要匹配和查找的范围，最终确定一个需要根据证书的特征信息进行匹配查找的子集，并根据接收到的证书的特征信息和吊销标识中包含的特征信息进行匹配，如果存在匹配的记录，则确定接收到的证书已被吊销，如果没有匹配的记录，则确定接收到的证书未被吊销。如果 CRL 中根本不存在接收到的证书的分类信息，则可以直接确定该接收到的证书未被吊销。

需要说明的是，本申请实施例中需要约定接收端接收到的证书的特征信息的定义，和 CRL 中吊销标识中记录的被吊销证书的特征信息定义保持一致。如果 CRL 中吊销标识中记录的被吊销证书的特征信息定义为被吊销证书标识中的指定位置的 n 个字节的随机数，则接收端在验证证书时从接收到的证书标识中提取指定位置的 n 个字节的随机数；如果 CRL 中吊销标识中记录的被吊销证书的特征信息定义为对被吊销证书进行哈希计算后截取指定位置的 n 个字节，则接收端在验证证书时对接收到的证书进行哈希计算后截取指定位置的 n 个字节。

通过如上实施例中所述的方法可以看出，通过在证书和 CRL 中吊销标识中包含分类信息，接受方在验证证书是否被吊销的时候，可以通过分类信息缩小需要查找和匹配的范围，在 CRL 中保存的记录较多的情况下，可以极大的减少接收端验证证书的计算量，提升验证证书的速度和效率，满足车联网中实时性的业务需求。

如图 2 实施例中所述，CRL 是证书吊销服务器生成的，图 4 所示为证书吊销服务器吊销证书，并在 CRL 中增加包含分类信息的吊销标识的方法流程示意图。

301-302、接收端接收车联网消息，其中包含消息发送端的证书，接收端判断存在异常情况，异常情况包括发送消息频率过快，消息中包含的签名信息验证错误，或证书不在有效期等，则将接收到的，包含证书的车联网消息发送给车联网服务器，请求车联网服务器做进一步安全性判断和处理。

303、车联网服务器接收到包含证书的车联网消息，根据本地策略进行判断和决策，确定需要对证书进行吊销，发送消息到证书吊销服务器，请求证书吊销服务器吊销该证书，消息中携带证书。需要说明的是，车联网服务器可以直接向证书吊销服务器发送消息，请求吊销证书，也可以通过证书颁发服务器向证书吊销服务器发送消息，请求吊销证书。如，当车联网服务器没有被授予写入证书吊销服务器的权限时，车联网服务器需要通过证书颁发服务器向证书吊销服务器发送消息。

304、证书吊销服务器根据车联网服务器的请求，在 CRL 中增加一条吊销标识记录，根据证书的格式，提取证书的分类信息和特征信息，并将该证书的分类信息写入新增的吊销标识。证书吊销服务器提取证书的分类信息的方式，与图 2 所示实施例中描述的携带分类信息的方式相对应。具体的，对应如图 2 所示实施例中描述的三种携带分类信息的方式，证书吊销服务器提取证书的 id 字段，或 region 字段，或 crlSeries 字段，中的分类信息，并将该分类信息作为 CRL 中新增的吊销标识字段的分类信息。证书吊销服务器提取证书的特征信息的方式，与图 2 所示实施例中描述的证书的格式相对应。当证书的某个约定字段，如 id 字段，中包含的 n 字节随机数作为证书的特征信息时，证书吊销服务器提取证书约定字段中的 n 字节随机数，作为被吊销证书的特征信息；其它情况下，或对证书进行哈希计算后截取 n 个字节，作为被吊销证书的特征信息。当吊销标识字段同时记录分类信息和特征信息时，按照“分类信息|被吊销证书的特征信息”的格式记录。

需要说明的是，当证书的特征信息和 CRL 中记录的被吊销证书的特征信息为哈希值时，接收端和证书吊销服务器所使用的哈希算法要保持一致。具体的，接收端在 102 步骤对接收到的证书进行哈希计算时所使用的哈希算法，和证书吊销服务器在 304 步骤对被吊销的证书进行哈希计算时所使用的哈希算法，保持一致。

可选的，证书吊销服务器在第 304 步执行的提取证书信息的方法，还可以由车联网服务器在第 303 步发送证书吊销请求之前执行，即作为第 303 步的替代方案，车联网服务器接收到包含证书的车联网消息，根据本地策略进行判断和决策，确定需要对证书进行吊销，车联网服务器提取证书的分类信息和特征信息，发送提取的证书的分类信息和特征信息到证书吊销服务器，请求证书吊销服务器吊销该证书。

如上结合图 4 中的步骤描述了在 CRL 中新增被吊销证书的流程。由于被吊销证书的记录是不断变化的，因此车联网通信单元从证书吊销服务器获取 CRL 后，还需要从证书吊销服务器获取 CRL 变化的信息，并更新本地存储的 CRL。

图 5 所示为本发明实施例提供的车联网通信单元获取 CRL 的方法流程示意图。车联网通信单元可以根据预设的触发条件主动向证书吊销服务器请求获取 CRL，如 401 步骤所示，还可以直接由证书吊销服务器根据预设的策略或规则向车联网通信单元广播或单播 CRL，即 402 消息即可以是 401 消息的响应，也可以是证书吊销服务器主动推送的消息。需要说明的是，车联网通信单元还可以间接从其它车联网通信单元获取 CRL，如 403 和 404 步骤所示，车联网通信单元 2 可以从已获取 CRL 的车联网通信单元 1 获取 CRL，404 消息可以是 403 请求的响应，也可以是车联网通信单元 1 主动通过广播或单播方式向车联网通信单元 2 推送的 CRL。

车联网通信单元主动请求获取 CRL 的触发条件可以是事件触发，如车辆点火启动，也可以是周期触发，如周期定时器超时，还可以是特定条件触发，如到达预订区域或预订速度阈值等。

证书吊销服务器或车联网通信单元在 402 或 404 消息中携带的 CRL 可以是全量 CRL，也可以是差分 CRL。所谓全量 CRL 包含证书吊销服务器吊销的所有证书的信息，差分 CRL 包括新

增 CRL 和删除 CRL 两个列表，其中新增 CRL 仅包括一个时间段内，时间段结束时间点对应的全量 CRL 相比时间段开始时间点对应的全量 CRL，新增的被吊销证书的信息，删除 CRL 仅包括一个时间段内，时间段结束时间点对应的全量 CRL 相比时间段开始时间点对应的全量 CRL，减少的被吊销证书的信息。如果采用差分更新的方案，则车联网通信单元在首次获取全量 CRL 后，后续在 402 或 404 消息中获取到的是差分 CRL，车联网通信单元需要根据新增 CRL 和删除 CRL 两个列表，刷新本地保存的 CRL；如果采用全量更新的方案，车联网通信单元在 402 或 404 消息中获取到的是全量 CRL，车联网通信单元将接收到的全量 CRL 直接替换本地保存的 CRL。

如上所述实施例描述了证书吊销服务器如何生成包含被吊销证书分类信息和特征信息的 CRL，车联网通信单元如何从证书吊销服务器获取包含被吊销证书分类信息和特征信息的 CRL，以及车联网通信单元在收到消息时，如何提取消息中证书的分类信息和特征信息，并与 CRL 中的记录进行匹配，以确定消息中携带的证书是否被吊销的方法。

由于车联网终端的数量巨大，车联网系统中颁发的证书数量也是海量的，相应的，被吊销证书的数量也相对较大。为降低保存被吊销证书的信息对车联网通信单元存储空间的影响，在上述 CRL 方案之外，本申请实施例进一步提出证书吊销指纹库方案。证书吊销指纹库为初始化为 0 的长度为 N 的二进制数组，证书吊销指纹库中记录了被吊销证书的指纹信息，被吊销证书的指纹信息为所述长度为 N 的二进制数组中取值为 1 的比特位信息，N 为大于 0 的正整数。被吊销证书的指纹信息可以通过多种算法对被吊销证书进行计算而获得，如可以采用哈希计算获得被吊销证书的指纹信息。

如图 6 所示，假设证书吊销指纹库为初始化为 0，长度为 16 的二进制数组。在图 4 所示流程的 304 步骤，当证书吊销服务器需要记录一个被吊销证书的时候，证书吊销服务器使用 3 个哈希函数，分别对被吊销证书进行哈希计算和映射（如用哈希计算的结果对指纹库二进制数组的长度取余），每次映射都会产生一个数值，每个数值对应二进制数组的一个比特位，将对应的比特位置为 1，这三个取值为 1 的比特位信息就是该被吊销证书的指纹信息。

图 2 所示的方法流程中，接收端收到包含证书的车联网消息，计算证书的指纹信息，并在证书吊销指纹库中进行匹配，如果有相同的指纹信息，则该证书已被吊销。需要说明的是，证书的格式可以是本申请实施例中所述的包含分类信息的格式，也可以是其它格式。

图 5 所示的方法流程中，车联网通信单元在 402 或 404 步骤获取到的是证书吊销指纹库。证书吊销指纹库可以是包含全部被吊销证书指纹信息的全量证书吊销指纹库，也可以是差分证书吊销指纹位置库，差分证书吊销指纹位置库记录了一个时间段内，时间段结束时间点对应的全量证书吊销指纹库相比时间段开始时间点对应的全量证书吊销指纹库，发生变化的比特位信息。

比如，证书吊销服务器中记录的全量证书吊销指纹库中包含两个被吊销证书 A 和 B 的指纹，指纹长度为 10，A 的指纹为 0010010001，B 的指纹为 0001110000，那么全量证书吊销指纹库为 0011110001。如果在 304 步骤要新增一个被吊销证书 C，假设 C 的指纹为 1100001000，则与总体指纹库 0011110001 对比，发现从右数第 4 比特，第 9 比特和第 10 比特的取值由 0 变为 1，则差分证书吊销指纹位置库中记录第 4 比特，第 9 比特和第 10 比特的取值发生变化，具体记录方式本申请不进行限定，可以以二进制数组的形式，将发生变化的比特位置为 1，也可以以枚举或数组的形式，只记录发生变化的比特位的序号。如果要从全量证书吊销指纹库中将 B 证书的指纹删除，则更新后的全量证书吊销指纹库为 0010010001，发生变化的比特位为从右数第 6 比特位和第 7 比特位，则差分证书吊销指纹位置库中记录第 6 比特和第 7 比

特的取值发生变化。

车联网通信单元如果收到差分证书吊销指纹位置库，则根据其中记录的比特位信息，将本地保存的证书吊销指纹库中对应的比特位的取值取反，就可以获得最新的证书吊销指纹库。如果收到全量证书吊销指纹库，则直接替换本地保存的证书吊销指纹库。

由于证书吊销指纹库中的 1 没有和特定的被吊销证书进行绑定，因此车联网通信单元在第 102 步骤进行证书验证的时候，可能会存在误判。如在证书吊销指纹库中记录的指纹信息较多的情况下，证书吊销指纹库中，一个待确认证书的指纹信息所对应的比特位可能都已被置为 1，而这些比特位并不一定对应同一个被吊销证书的指纹。

作为发送端的车联网通信单元，在 101 步骤发送消息前，为防止接收端误判而丢弃自己发送的消息，首先使用本地保存的证书吊销指纹库，自行验证证书的指纹信息是否在证书吊销指纹库中有匹配的记录，确保在消息中携带一个在证书吊销指纹库中没有匹配记录的证书，如图 7 中 100 步骤所示。一般情况下，证书颁发服务器会一次颁发给车联网通信单元多个证书，车联网通信单元在这些证书中，选用一个在证书吊销指纹库中没有匹配记录的证书。如果本地没有可用的证书，则车联网通信单元重新向证书颁发服务器申请证书。

作为接收端的车联网通信单元，在 102 步骤，如果确定消息中证书的指纹信息在证书吊销指纹库中存在，为了防止误判，请求证书吊销服务器验证证书，如图 8 中 103 步骤所示，请求消息中包含证书或证书的信息。由于证书吊销服务器不仅保存了被吊销证书的指纹信息，还保存了 CRL 等信息，因此证书吊销服务器的验证结果更加准确。接收端的车联网通信单元最终以证书吊销服务器在 104 步骤中返回的验证结果为准，对 V2X 消息进行处理。如果证书吊销服务器返回的验证结果为未吊销，则接收端继续处理 V2X 消息；如果证书吊销服务器返回的验证结果为已吊销，则接收端丢弃 V2X 消息。

本申请实施例中所述的证书吊销列表方案和证书吊销指纹库方案，都是为了提升车联网通信中，车联网终端或车联网通信单元验证证书的效率和速度，以提升消息处理的实时性，并降低验证证书对车联网终端或车联网通信单元性能的影响。相比证书吊销列表方案，证书吊销指纹库方案对车联网终端或车联网通信单元存储空间的要求更低，车联网终端或车联网通信单元保存证书吊销指纹库只需要占用很少的存储空间，但另一方面，证书吊销指纹库方案可能存在一定的误判概率，因此除了接收端进行证书的验证，还需要额外的处理以提升证书验证的准确性。

需要说明的是，证书吊销列表方案和证书吊销指纹库方案可以各自独立应用，也可以组合应用。两种方案组合应用时，证书的格式采用证书吊销列表方案中描述的包含分类信息的格式，证书吊销服务器同时保存 CRL 和证书吊销指纹库，车联网通信单元只保存证书吊销指纹库。两种方案组合应用的场景下：

304 步骤，证书吊销服务器同时根据证书吊销列表方案和证书吊销指纹库方案分别刷新 CRL 和证书吊销指纹库；

402 步骤或 404 步骤，车联网通信单元只获取并保存证书吊销指纹库，以减少对存储空间的消耗；

102 步骤，车联网通信单元采用证书吊销指纹库方案对证书进行验证；

103-104 步骤，为提高验证的准确性，车联网通信单元请求证书吊销服务器对证书进行验证，证书吊销服务器使用 CRL 列表对证书进行快速验证。

上述主要从方法流程的角度对本发明实施例提供的方案进行了介绍。可以理解的是，车联网通信单元、车联网服务器和证书吊销服务器等实体为了实现上述功能，其包含了执行各

个功能相应的硬件结构和/或软件模块。另外，本申请实施例中所描述的车联网服务器和证书吊销服务器可以是分离的物理设备，也可以是同一个物理设备中的不同逻辑功能实体，即本申请实施例中车联网服务器和证书吊销服务器所具备的功能可以在同一个物理设备中实现。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的方法流程，本发明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发明的范围。

例如，如上实施例中的车联网通信单元、车联网服务器和证书吊销服务器均可以由如图 9 所示的装置来实现。

装置 500 包括至少一个处理器 501，通信总线 502，存储器 503 以及至少一个通信接口 504。

处理器 501 可以是一个通用中央处理器（central processing unit，CPU），微处理器，特定应用集成电路（application-specific integrated circuit，ASIC），或一个或多个用于控制本发明方案程序执行的集成电路。

通信总线 502 可包括一通路，在上述组件之间传送信息。

通信接口 504，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，无线接入网（radio access network，RAN），无线局域网(wireless local area networks，WLAN)等。

存储器 503 可以是只读存储器（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，随机存取存储器（random access memory，RAM）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。存储器可以是独立存在，通过总线与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 503 用于存储执行本发明方案的应用程序代码，并由处理器 501 来控制执行。处理器 501 用于执行存储器 503 中存储的应用程序代码，从而实现本专利方法中车联网通信单元、车联网服务器和证书吊销服务器的功能。

在具体实现中，作为一种实施例，处理器 501 可以包括一个或多个 CPU，例如图 6 中的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，装置 500 可以包括多个处理器，例如图 6 中的处理器 501 和处理器 508。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器。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。

在具体实现中，作为一种实施例，装置 500 还可以包括输出设备 505 和输入设备 506。输出设备 505 和处理器 501 通信，可以以多种方式来显示信息。例如，输出设备 505 可以是液晶显示器（liquid crystal display，LCD），发光二级管（light emitting diode，LED)显示设备，阴极射线管（cathode ray tube，CRT）显示设备，或投影仪（projector）等。输入设备 506 和处理器 501 通信，可以以多种方式接受用户的输入。例如，输入设备 506 可以是鼠标、键盘、触摸屏设备或传感设备等。

当上述装置实现车联网服务器或证书吊销服务器的功能时，装置 500 可以是一个通用服

务器或者是一个专用服务器。

当上述装置实现本申请实施例中车联网通信单元的功能时，装置 500 可以是集成在车辆中的车载盒子（Telematics BOX，T-Box）或多域控制器（Multi-Domian Controller，MDC）。可选的，可选的，装置 500 还可以是集成在车辆中的芯片，那么通信接口 504 的功能/实现过程还可以通过管脚或电路等来实现；所述存储器为所述芯片内的存储单元，如寄存器、缓存等，所述存储单元还可以是位于所述芯片外部的存储单元。

在上述实施例中，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发明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、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（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能够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，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk (SSD)）等。

以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，本领域技术人员应该理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。在权利要求中，“包括”一词不排除其他组成部分或步骤，“一”或“一个”不排除多个的情况。单个处理器或其它单元可以实现权利要求中列举的若干项功能。相互不同的从属权利要求中记载了某些措施，但这并不表示这些措施不能结合起来产生良好的效果。

权 利 要 求 书

1、一种确定证书状态的方法，其特征在于，

接收端接收发送端发送的消息，所述消息中包括所述发送端证书，所述发送端证书中包含分类信息；

所述接收端根据所述分类信息，在保存的证书吊销列表中确定吊销标识的集合，所述吊销标识用于在所述证书吊销列表中标识被吊销证书，所述吊销标识包含被吊销证书的分类信息，所述集合中的吊销标识包含的分类信息与所述发送方证书的分类信息相同；

所述接收端提取所述发送端证书的特征信息，与所述集合中吊销标识对应的被吊销证书的特征信息进行匹配，并根据匹配结果确定所述发送端证书的状态。

2、根据权利要求 1 所述的方法，其特征在于，所述吊销标识包含的特征信息为所述吊销标识对应的被吊销证书的第一约定字段包含的 N 个字节的随机数，N 为大于 0 的正整数；

所述接收端提取所述发送端证书的特征信息，具体包括：

所述接收端从所述发送端证书的第一约定字段截取 N 个字节的随机数作为所述发送端证书的特征信息。

3、根据权利要求 1 所述的方法，其特征在于，所述吊销标识包含的特征信息为对所述吊销标识对应的被吊销证书进行哈希运算后得到的 M 个字节的哈希值，M 为大于 0 的正整数；

所述接收端提取所述发送端证书的特征信息，具体包括：

所述接收端对所述发送端证书进行所述哈希运算后，得到的 M 个字节的哈希值作为所述发送端证书的特征信息。

4、根据权利要求 1-3 任一所述的方法，其特征在于，所述发送端证书的分类信息包含在所述发送端证书的第二约定字段中。

5、根据权利要求 4 所述的方法，其特征在于，所述第二约定字段为所述发送端证书的证书标识字段，或所述证书的区域字段，或所述证书的证书吊销系列字段。

6、根据权利要求 1-5 任一所述的方法，其特征在于，所述分类信息包含第一级分类信息和第二级分类信息。

7、根据权利要求 6 所述的方法，其特征在于，

所述接收端根据所述分类信息，在保存的证书吊销列表中确定吊销标识的集合，具体包括：

所述接收端根据所述发送端证书的第一级分类信息，在所述证书吊销列表中确定第一吊销标识的集合，所述第一吊销标识的集合中的吊销标识包含的的第一级分类信息与所述发送端证书的第一级分类信息相同；

所述接收端根据所述发送端证书的第二级分类信息，在所述第一吊销标识的集合中确定第二吊销标识的集合，所述第二吊销标识的集合中的吊销标识包含的的第二级分类信息与所述发送端证书的第二级分类信息相同。

8、根据权利要求 1-7 任一所述的方法，其特征在于，所述接收端根据所述分类信息，在保存的证书吊销列表中确定吊销标识的集合之前，所述方法还包括，所述接收端从证书吊销服务器获取证书吊销列表。

9、根据权利要求 8 所述的方法，其特征在于，所述接收端从证书吊销服务器获取证书吊销列表具体包括，

所述接收端从证书吊销服务器获取全量证书吊销列表；

所述接收端从证书吊销服务器获取差分证书吊销列表，所述差分证书吊销列表包括一个

新增证书吊销列表和一个删除证书吊销列表，所述新增证书吊销列表中包括相比所述全量证书吊销列表，增加的吊销标识，所述删除证书吊销列表中包括相比所述完整的证书吊销列表，删除的吊销标识；

所述接收端根据所述差分证书吊销列表，刷新保存的所述全量证书吊销列表。

10、根据权利要求 1-9 任一所述的方法，其特征在于，所述接收端根据匹配结果确定所述发送端证书的状态，具体包括，

所述接收端在通过匹配，确定所述集合中吊销标识对应的被吊销证书的特征信息中，存在与所述发送端证书的特征信息相同的特征信息，则所述接收端确定所述发送端证书已被吊销。

11、根据权利要求 1-9 任一所述的方法，其特征在于，所述接收端根据匹配结果确定所述发送端证书的状态，具体包括，

所述接收端通过匹配，确定所述集合中吊销标识对应的被吊销证书的特征信息中，不存在与所述发送端证书的特征信息相同的特征信息，则所述接收端确定所述发送端证书未被吊销。

12、根据权利要求 1-11 任一所述的方法，其特征在于，所述接收端或发送端为车载通信单元或路侧通信单元。

13、一种确定证书状态的方法，其特征在于，

接收端接收发送端发送的消息，所述消息中包括所述发送端证书；

所述接收端确定证书吊销指纹库中存在与所述发送端证书的指纹信息匹配的被吊销证书的指纹信息，所述发送端证书的指纹信息为所述接收端根据所述发送端证书计算获得；

所述接收端向证书吊销服务器发送所述发送端证书，请求所述证书吊销服务器验证所述发送端证书的状态；

所述接收端接收所述证书吊销服务器的验证结果，并根据所述验证结果确定所述发送端证书的状态。

14、根据权利要求 13 所述的方法，其特征在于，所述证书吊销指纹库为初始化为 0 的长度为 N 的二进制数组，所述指纹信息为长度为 N 的二进制数组中取值为 1 的比特位信息，N 为大于 0 的正整数。

15、根据权利要求 13 或 14 所述的方法，其特征在于，所述接收端对所述发送端证书进行哈希运算，对哈希运算后的取值截取其中 M 个字节，M 为大于 0 的正整数，对所述 M 个字节的数值进行哈希运算并对 N 取模，获得所述发送端证书的指纹信息。

16、根据权利要求 13-15 任一所述的方法，其特征在于，所述接收端接收发送端发送的消息之前，所述方法还包括，所述接收端从证书吊销服务器或第三车联网通信单元获取所述证书吊销指纹库。

17、根据权利要求 16 所述的方法，其特征在于，所述接收端从证书吊销服务器或第三车联网通信单元获取所述证书吊销指纹库，具体包括，

所述接收端从证书吊销服务器或第三车联网通信单元获取全量证书吊销指纹库，所述全量证书吊销指纹库中包括所有被吊销证书的指纹信息；

所述接收端从证书吊销服务器或第三车联网通信单元获取差分证书吊销指纹位置库，所述差分证书吊销指纹位置库记录所述全量证书吊销指纹库发生变化的比特位信息；

所述接收端根据所述差量证书吊销指纹库，将所述全量证书吊销指纹库中发生变化的比

特位对应的取值进行取反运算。

18、根据权利要求 13-17 任一所述的方法，其特征在于，所述接收端确定所述发送端证书被吊销的情况下，所述方法还包括，所述接收端丢弃所述发送端发送的消息。

19、根据权利要求 13-18 任一所述的方法，其特征在于，所述接收端或发送端或第三车联网通信单元为车载通信单元或路侧通信单元。

20、一种确定证书状态的方法，其特征在于，

证书吊销服务器接收请求吊销证书的消息，所述请求吊销证书的消息中包括证书，所述证书中包含所述证书的分类信息；

所述证书吊销服务器提取所述证书的分类信息和特征信息，并在证书吊销列表中记录所述证书的分类信息和特征信息。

21、根据权利要求 20 所述的方法，其特征在于，所述证书的特征信息为所述证书的第一约定字段包含的 N 个字节的随机数，N 为大于 0 的正整数；

所述证书吊销服务器提取所述证书的特征信息，具体包括：

所述证书吊销服务器在所述证书的第一约定字段截取 N 个字节的随机数作为所述证书的特征信息。

22、根据权利要求 20 所述的方法，其特征在于，所述证书的特征信息为对所述证书进行哈希运算后得到的 M 个字节的哈希值，M 为大于 0 的正整数；

所述证书吊销服务器提取所述证书的特征信息，具体包括：

所述证书吊销服务器对所述证书进行所述哈希运算后，得到的 M 个字节的哈希值作为所述证书的特征信息。

23、根据权利要求 20-22 任一所述的方法，其特征在于，所述证书的分类信息包含在所述证书的第二约定字段中；

所述证书吊销服务器提取所述证书的分类信息，具体包括：

所述证书吊销服务器在所述证书的第二约定字段截取所述证书的分类信息。

24、根据权利要求 23 所述的方法，其特征在于，所述第二约定字段为所述证书的证书标识字段，或所述证书的区域字段，或所述证书的证书吊销系列字段。

25、根据权利要求 20-24 任一所述的方法，其特征在于，所述证书吊销服务器在所述证书吊销列表中的吊销标识字段记录所述证书的分类信息。

26、根据权利要求 20-25 任一所述的方法，其特征在于，所述证书吊销服务器在所述证书吊销列表中的吊销标识字段记录所述证书的特征信息。

27、根据权利要求 20-26 任一所述的方法，其特征在于，所述证书吊销服务器将所述证书的分类信息和所述证书的特征信息进行连接运算，并在所述证书吊销列表中的吊销标识字段记录所述连接运算后得到的值。

28、一种确定证书状态的方法，其特征在于，

证书吊销服务器接收车联网服务器发送的请求吊销证书的消息，所述请求吊销证书的消息中包括证书；

所述证书吊销服务器计算获得所述证书的指纹信息，并在证书吊销指纹库记录所述证书的指纹信息；

所述证书吊销服务器比较证书吊销指纹库记录所述证书的指纹信息前后发生变化的比特

位信息，并将发生变化的比特位信息记录到差分证书吊销指纹位置库。

29、根据权利要求 28 所述的方法，其特征在于，所述证书吊销指纹库中包括被吊销证书的指纹信息，所述证书吊销指纹库为初始化为 0 的长度为 N 的二进制数组，所述指纹信息为长度为 N 的二进制数组中取值为 1 的比特位信息，N 为大于 0 的正整数。

30、根据权利要求 28 或 29 所述的方法，其特征在于，所述方法还包括，所述证书吊销服务器向车联网通信单元发送所述差分证书吊销指纹位置库。

31、一种确定证书状态的方法，其特征在于，

车联网服务器接收第一车联网通信单元发送的消息，所述消息中包括第二车联网通信单元发送给所述第一车联网通信单元的消息，所述第二车联网通信单元发送给所述第一车联网通信单元的消息中包括所述第二车联网通信单元的证书，所述证书中包括所述证书的分类信息；

所述车联网服务器提取所述的证书的分类信息和特征信息；

所述车联网服务器向证书吊销服务器发送消息，请求吊销所述证书，所述消息中包括所述证书的分类信息和特征信息。

32、根据权利要求 31 所述的方法，其特征在于，所述证书的特征信息为所述证书的第一约定字段包含的 N 个字节的随机数，N 为大于 0 的正整数；

所述车联网服务器提取所述第二车联网通信单元的证书的特征信息，具体包括：

所述车联网服务器在所述证书的第一约定字段截取 N 个字节的随机数作为所述证书的特征信息。

33、根据权利要求 31 所述的方法，其特征在于，所述证书的特征信息为对所述证书进行哈希运算后得到的 M 个字节的哈希值，M 为大于 0 的正整数；

所述车联网服务器提取所述第二车联网通信单元的证书的特征信息，具体包括：

所述车联网服务器对所述证书进行所述哈希运算后，得到的 M 个字节的哈希值作为所述证书的特征信息。

34、根据权利要求 31-33 任一所述的方法，其特征在于，所述证书的分类信息包含在所述证书的第二约定字段中；

所述车联网服务器提取所述第二车联网通信单元的证书的分类信息，具体包括：

所述车联网服务器在所述证书的第二约定字段截取所述证书的分类信息。

35、根据权利要求 34 所述的方法，其特征在于，所述第二约定字段为所述证书的证书标识字段，或所述证书的区域字段，或所述证书的证书吊销系列字段。

36、根据权利要求 31-35 任一所述的方法，其特征在于，所述分类信息包含第一级分类信息和第二级分类信息。

37、根据权利要求 31-36 任一所述的方法，其特征在于，所述第一车联网通信单元或第二车联网通信单元为车载通信单元或路侧通信单元。

38、一种车联网通信单元，其特征在于，包括：通信接口、存储器和处理器，

所述通信接口用于与车联网通信单元外部的装置或设备进行通信；

所述存储器用于存储程序；

所述处理器用于执行所述存储器中存储的程序，当所述程序被执行时，所述车联网通信单元执行如权利要求 1-19 任一所述的方法。

39、一种证书吊销服务器，其特征在于，包括：通信接口、存储器和处理器，

所述通信接口用于与证书吊销服务器外部的装置或设备进行通信；

所述存储器用于存储程序；

所述处理器用于执行所述存储器中存储的程序，当所述程序被执行时，所述证书吊销服务器执行如权利要求 20-30 任一所述的方法。

40、一种车联网服务器，其特征在于，包括：通信接口、存储器和处理器，

所述通信接口用于与车联网服务器外部的装置或设备进行通信；

所述存储器用于存储程序；

所述处理器用于执行所述存储器中存储的程序，当所述程序被执行时，所述车联网服务器执行如权利要求 31-37 任一所述的方法。

41、一种计算机可读存储介质，其特征在于，包括计算机指令，当所述计算机指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 37 中任一项所述的方法。

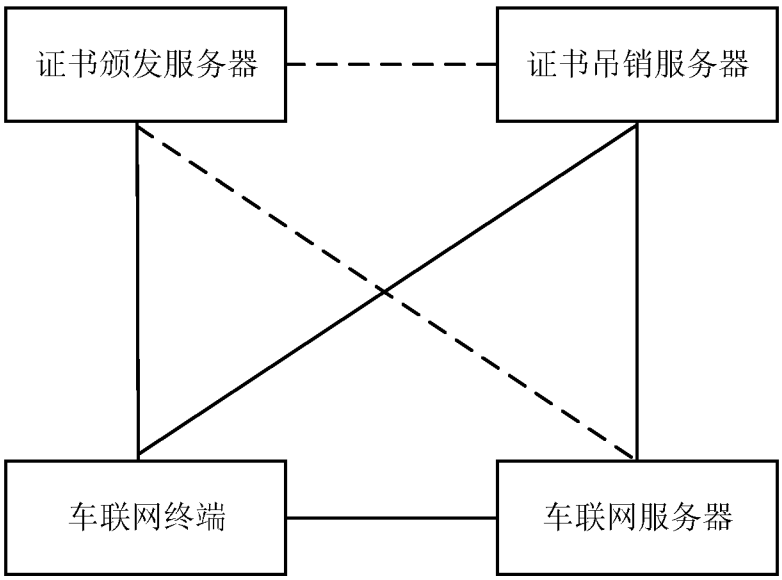

证书颁发服务器
证书吊销服务器
车联网终端
车联网服务器

图 1

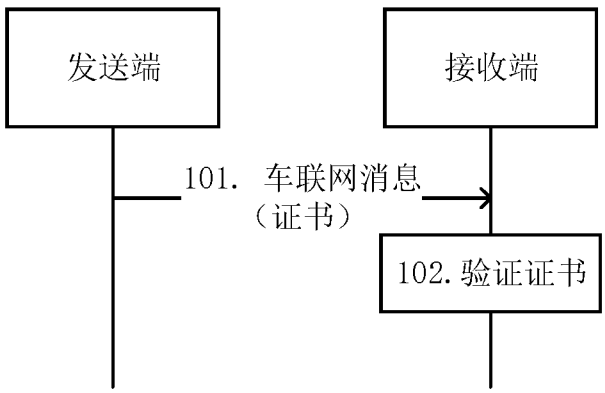

发送端
接收端
101. 车联网消息
（证书）
102. 验证证书

图 2

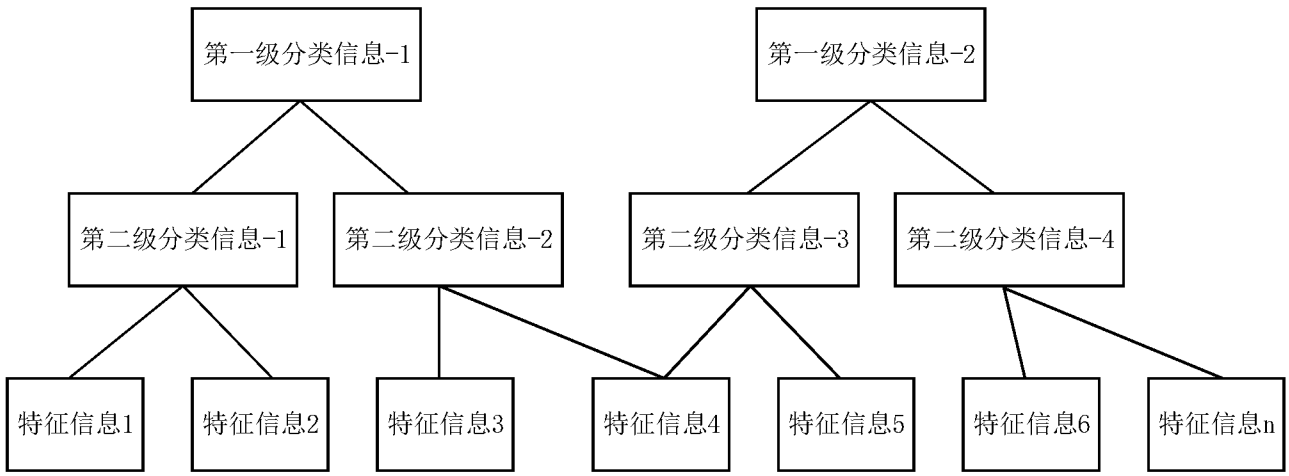

第一级分类信息-1
第一级分类信息-2
第二级分类信息-1
第二级分类信息-2
第二级分类信息-3
第二级分类信息-4
特征信息1
特征信息2
特征信息3
特征信息4
特征信息5
特征信息6
特征信息n

图 3

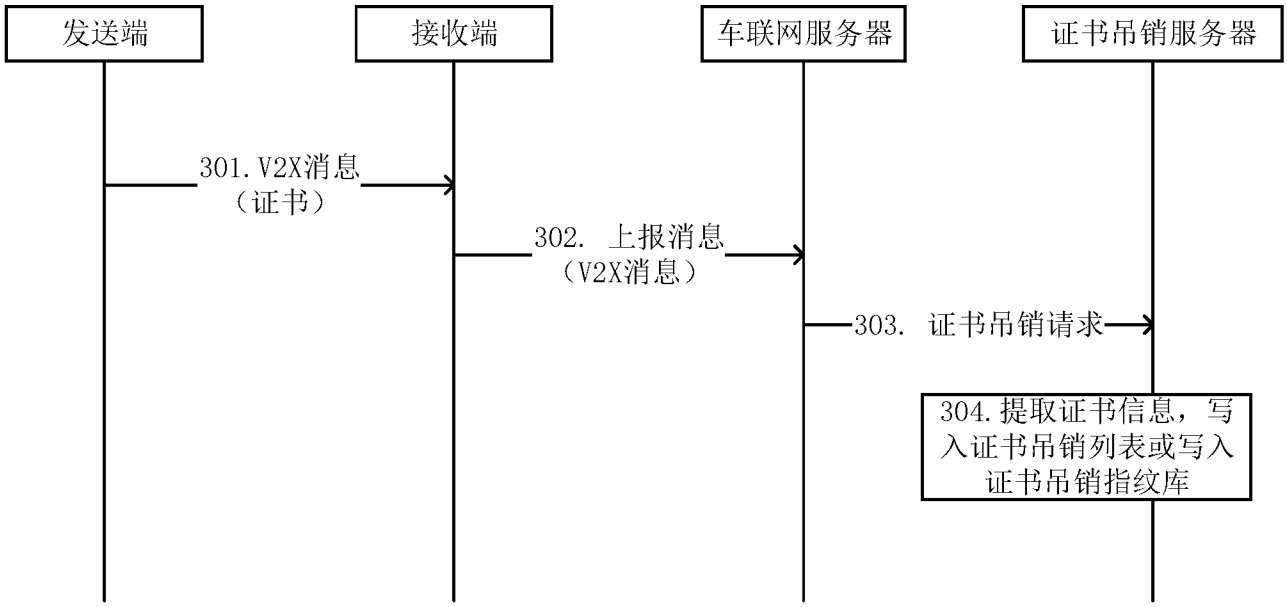

发送端
接收端
车联网服务器
证书吊销服务器
301. V2X消息
（证书）
302. 上报消息
（V2X消息）
303. 证书吊销请求
304. 提取证书信息，写入证书吊销列表或写入证书吊销指纹库

图 4

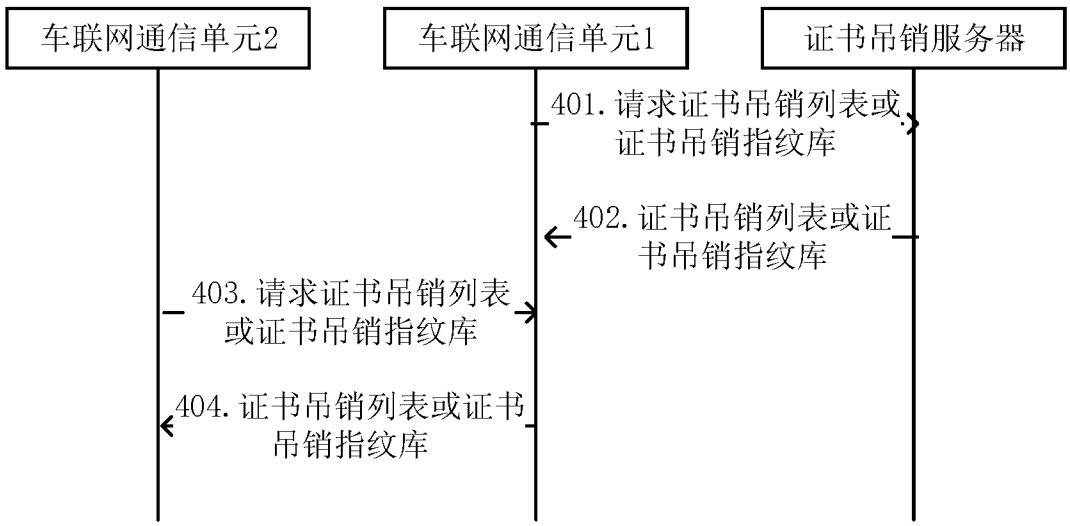

车联网通信单元2
车联网通信单元1
证书吊销服务器
401. 请求证书吊销列表或证书吊销指纹库
402. 证书吊销列表或证书吊销指纹库
403. 请求证书吊销列表或证书吊销指纹库
404. 证书吊销列表或证书吊销指纹库

图 5

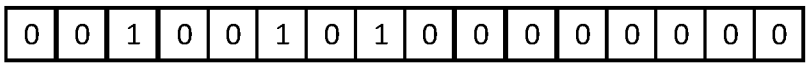

0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0

图 6

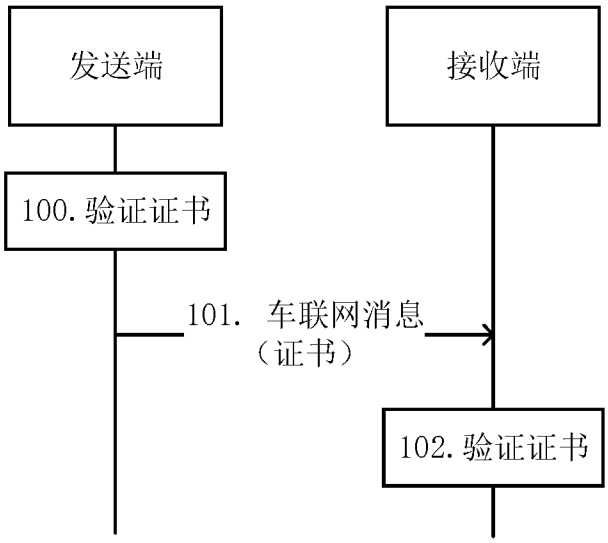

发送端
接收端
100. 验证证书
101. 车联网消息
（证书）
102. 验证证书

图 7

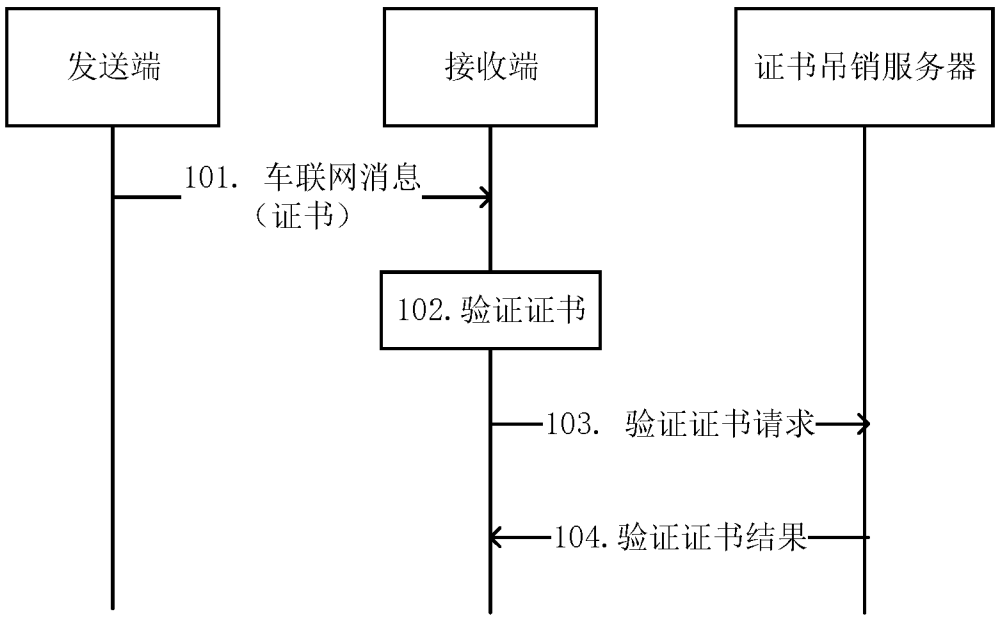

发送端
接收端
证书吊销服务器
101. 车联网消息
（证书）
102. 验证证书
103. 验证证书请求
104. 验证证书结果

图 8

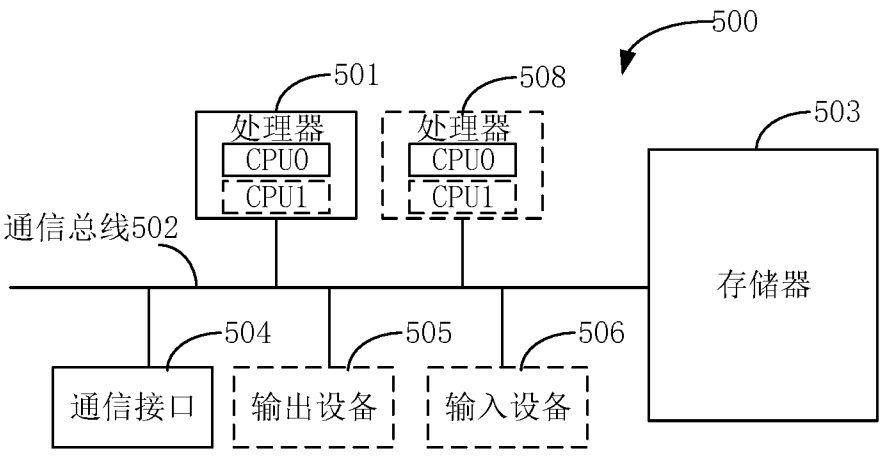

500
501
508
处理器
CPU0
CPU1
处理器
CPU0
CPU1
503
通信总线502
存储器
504
505
506
通信接口
输出设备
输入设备

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/098056

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNABS; CNTXT; CNKI; EPTXT; WOTXT; USTXT; VEN; 3GPP: 吊销, 分类, 证书,证书, 验证, 车, 车联, 路测单元, 网联汽车车载通信单元,在线证书状态协议, revoke, withdraw, cancel+, class+, certificate, validate, verif+, vehicle, V2X, Vehicle-to-Everything, RSU, road side unit, on-board-unit, OBU, OCSP, Online Certificate Status Protocol

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108092777 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 29 May 2018 (2018-05-29) description, paragraphs 24-33	20-27, 31-37, 39-41
A	CN 107786515 A (CHINA MOBILE GROUP DESIGN INSTITUTE CO., LTD. ET AL.) 09 March 2018 (2018-03-09) entire document	1-41
A	CN 102236753 A (ZTE CORPORATION) 09 November 2011 (2011-11-09) entire document	1-41
A	CN 107508682 A (NUBIA TECHNOLOGY CO., LTD.) 22 December 2017 (2017-12-22) entire document	1-41
A	EP 3226464 A1 (SIEMENS AG) 04 October 2017 (2017-10-04) entire document	1-41

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 September 2019	**18 October 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/098056

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108092777 A	29 May 2018	None	
CN 107786515 A	09 March 2018	None	
CN 102236753 A	09 November 2011	CN 102236753 B	08 June 2016
CN 107508682 A	22 December 2017	None	
EP 3226464 A1	04 October 2017	DE 102016205203 A1	05 October 2017
		US 2017288880 A1	05 October 2017
		EP 3226464 B1	28 August 2019

国际检索报告

国际申请号
PCT/CN2019/098056

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CPRSABS;CNABS;CNTXT;CNKI;EPTXT;WOTXT;USTXT;VEN;3GPP:吊销，分类，证书,证书，验证， 车，车联，路测单元，网联汽车车载通信单元,在线证书状态协议, revoke, withdraw, cancel+, class+, certificate, validate, verif+, vehicle, V2X, Vehicle-to-Everything, RSU, road side unit, on-board-unit, OBU,OCSP,Online Certificate Status Protocol

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 108092777 A (北京奇虎科技有限公司) 2018年 5月 29日 (2018-05-29) 说明书24-33段	20-27, 31-37, 39-41
A	CN 107786515 A (中国移动通信有限公司研究院等) 2018年 3月 9日 (2018-03-09) 全文	1-41
A	CN 102236753 A (中兴通讯股份有限公司) 2011年 11月 9日 (2011-11-09) 全文	1-41
A	CN 107508682 A (努比亚技术有限公司) 2017年 12月 22日 (2017-12-22) 全文	1-41
A	EP 3226464 A1 (SIEMENS AG) 2017年 10月 4日 (2017-10-04) 全文	1-41

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 9月 26日	2019年 10月 18日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	毛韵楠
传真号 (86-10)62019451	电话号码 86-(010)-62089144

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/098056

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108092777	A	2018年 5月 29日	无			
CN	107786515	A	2018年 3月 9日	无			
CN	102236753	A	2011年 11月 9日	CN	102236753	B	2016年 6月 8日
CN	107508682	A	2017年 12月 22日	无			
EP	3226464	A1	2017年 10月 4日	DE	102016205203	A1	2017年 10月 5日
				US	2017288880	A1	2017年 10月 5日
				EP	3226464	B1	2019年 8月 28日