### 3.1.2 云层

本章中我们主要介绍了云层，云层由两部分组成，第一部分是中心云，第二部分是本地云。

（1）中心云：详见图 2-2。中心云由三个数据库构成，第一个数据库是车辆注册数据库，假名数据库及全局认证中心。第二个数据库是注册数据，主要负责存储车辆的车牌号码，车主的信息，以及车主的住址等等，根据这些匹配信息，深层映射表保存［１６］。第三个数据库叫假名数据库，其主要功能是，定期的产生假名，且进行储存。这些假名需要注册数据库完成后期的记录工作，并做好备案，并不按规则的分发到本地云中。为了确保假名的高效管理，我们在全局认证中心，增加了匹配车辆的认证信息。

（2）（2）本地云： 本地云主要是有一些位置相近的路测单元构成。在本地云中，有假名池，路侧单元，事件记录器以及本地认证中心。其中假名池的主要作用是存储假名，这些假名主要是由中心云假名数据库分配得到的，为了更好的记录这些信息，假名池需要独立创建一个空列表，并将假名与本地云进行一一匹配。一般来说，其基本的工作步骤是，本地云不按规则的分发假名，并通过分辨系统识别出合法车辆，分配对应的假名公钥，以及假名私钥。路侧单元记录主要是负责，记录路侧单元的信息，有些路侧单元都来自同样的本地云。事件纪录器的功能比较强大，不仅负责记录车辆破坏行为、路侧单元的破坏行为，还要对本地语言进行实时的跟踪监察。本地认证中心主要负责最后的认证信息传送工作，最终全局认证中心接收到该信息。本地云通信的方式主要有两种，一种是通过有线方式，总是通过无线方式。

### 3.1.3 用户层

一般而言，驾驶者的社交行为方式一般可以决定车辆的移动特性，从而间接地对区域的假名管理工作产生作用。为了发现车辆时空分布的规律，主要研究了实际行驶轨迹的数据集 ［９４］，挖掘车辆时空分布特性， 本章总结车辆运动主要具有以下规律本章主要介绍了车辆的运动规律，具体有以下几个方面［１６］ ［８７］：

（1）道路的状况会影响车辆的运动轨迹。 拿系统来说， 在道路中有许多的交叉路口，这些地点也是系统社交的中心。对一辆车而言，所谓个人社交热点，就是车辆经过频率最多的地点，比如离车主家最近的十字路口，也可以称之为热点。一般而言，同一个社交热点可以对应许多车辆。举例来说，在同一个公司里，该公司的停车场也是所有工作人员车辆社交热点。由上文的介绍可以知道，如果一个地点，同时作为多

辆车的社交热点，也可以称之为全局的社交热点。

（2）根据经验来说， 绝大多数的车辆都会经过各自的个人社交热点， 在每个工作日中，经过社交热点的时间间隔，我们发现这些间隔十分小。造成这一规律的主要原因是，车主的交际往来一般来说是比较固定的１９５］ 。以上发现说明， 车辆带有多种属性，它不仅仅体现着驾驶员的交际特点，还体现着多个驾驶人员共同的交际特点。借助这一发现，在本章中，设计出一个高校的假名分发管理系统。

## 3.2 假名分发系统

### 3.2.1 假名分发方案

由于车辆 vi，是在移动云技术的基础上设计出的，因此可以得到全局认证中心的认可，获得长期身份证书。这一长期身份证书相当于人类的身份证号码，主要是因为在这张身份证输上，编入了车辆的一系列信息。车辆的假名产生的过程如下，产生假名的工作主要是由全局认证中心来完成，产生之后，假名会被存放在假名数据库中，随后，由全局认证中心抽取假名，抽取的数量不受限制，抽取的方式也没规律，并将这些假名放在一个集合内，并将这一集合传送至本地云。车辆申请假名的具体步骤如下，车辆应该按照行程计划，在形成之前，进行假名申请的工作，是由于这一机理，保证了车辆使用已有假名的稳定性。在申请假名的时候，第一步应该。上传车辆的长期身份证书，并由全局认证中心负责对证书进行审核，证书的合格主要依据假名集合进行判断。如果审核不合格，那么全局认证中心就会识别出这辆车的真实信息，并将这辆车假名列入禁区。而且，这辆违规车辆也会被上传到全局认证中心，由全局认证中心通知全部的车辆 。

借助路侧单元，车辆完成了假名申请工作，并最终，本地云接收到请求。如图 2-3，描绘了信息交互的具体过程，这一过程发生在车辆进行假名申请，以及地云接收到请求并发生系列指令，全过程中，包括协议一这一过程，表 2－1，列出了这一过程所运用的绝大部分符号。以下是车辆如何完成假名请求的介绍 ：

第一步，借助最近路侧单元，全局认证中心，定时的发布信息系统，传送至周围的车辆。其中，服务系统包括以下几个部分，第一部分是具体提供的服务、第二部分是地理位置范围、第三部分是本地云的位置、第四部分是全局认证中心相关信息、第五部分则是本 地云的身份资料等。

第二步：车辆 Vi，进入本地云 Lcn 的覆盖范围后，由 vi 负责接受服务信息，并经过后期的处理，对 Infor_service 做出真为判断。完成这一工作之后，全局认证中心将分配给该车辆一个公钥，对车辆申请的假名请求，以及 该车辆的身份资料，进行加密

处理，完成加密后， 协议一中的假名 request便生成成功。这一步骤十分重要，可以保证信息的安全性，阻止第三方的攻 击。除此之外，借助于最近的路测单元，会给每个车辆分配一个数字签名，并最终会传送至本地认证中心。

步骤 3：本地认证中心收到来至车辆 vi 的请求后， 并借助其从全局认证中心所取得的公钥，完成加密处理之后 ，将对应的信息提炼出来，然后本地认证中心提取其中的数字签名，最后附上数字签名，最后完成信息的输送。

第四步 :全局认证中心接收该信息后，对该信息进行一定的处理，这部分的工作主要是由注册数据库来完成，意思来检验车辆的身份信息，与此同时，并对全民的假名黑名单进行搜索，来排检车辆。完成以上操作后，将检验的信息打包，并传送给本地认证中心。

第五步，完成信息传输后，如果反馈信息表明，该车辆 vi 通过检测，那么本地认证中心将会授予该车辆假名，否则，会拒绝汽车所提出的假名申请。如果出现这样一种情况，此时假名池中存在着大量的假名，并且车辆 vi 也是合法车辆，这时本地认证中心，会给车辆发送一组由假名集合组成的信息，该集合主要包括匹配车辆的公钥以及私钥，还包括假名证书。

### 3.2.2 问题求解

在本节的介绍中，假名十分重要，它负责全局认证，以及本地认证管理。全区认证中心，负责整理假名的工作，其将假名打包成几个不同的集合，并依次生成一个列表，被处理后的假名根据列表类型便会分配到不同本地云的假名池中，列表主要包括以下信息，假名的身份信息，总数，假名的接收者等。

假设假名的产 生速度为 θ 。假设本地云需要 m 个假名。为了保证位置信息安全性，对车辆的假名数量提出了要求。我们可以通过计算该车辆的社交热点的车辆所需要假名的数目，来估计，该车辆在特定的时间内所需要的假名数量。经过一个时间间隔之后，中心云通过估计的 $D^{t}_{i}$，分发一定量的假名给 $LC_i$。其中估计的假名需求变量，会随着时间的变化而变化，并且可以通过车辆的移动记录，分析出规律，以此获得概率密度分布函数？ $(D^{t}_{i})$。

在本节中，我们运用了报童模型，来确定本地云与车辆之间的假名分配［96］。在以前的模型里，抱团负责供给资源，负责将报纸分发给对应的客户。在我们的假名分发模型中，本地云所扮演的功能就相当于报童，假名就如同传统模型中的报纸，车辆就是传统模型中的客户。不同的假名数目会影响运行的效率，关于假名树木的选择主要由本地云来完成，有本地云发出的假名数请求记为 $Q^{t}_{i}$。如果 $Q^{t}$ 小于 $D^{t}_{i}$，那么分发假名的时候，本地云 $LC_i$ 便可以得到好处，我们用 e 来表示。否则，在

本地云 $LC_i$ 中，剩余的假名 $(Q^t_i - D^t_i)$将会被存放在假名池中，在存放过程中，也会产生存储费用，我们用 s 来表示。如果 $LC_i$ 不能达到本地车辆的要求，作为对 $LC_i$ 的惩罚，将会被罚款，罚款的金额用屁来表示， $LC_i$ 的效益函数为：

$$u^t_i=\min\{D^t_i,Q^t_i\}*e-\max\{(Q^t_i - D^t_i),0\}*s-\max\{(D^t_i-Q^t_i)\}*P, \quad (2\text{-}1)$$

为了简化，我们令 $x^+ = \max(x, 0)$，并把（2-1）式子该写为

$$u^t_i = (e+p)Q^t_i-(e+p+s)(Q^t_i - D^t_i) - pD^t_i. \quad (2\text{-}2)$$

利用 $D^t_i$ 的时变特性，处理 （2-2）式子得

$$u^t_i = (e+p)Q^t_i - (e+p+s)(Q^t_i - D^t_i) \int_0^{Q^t_i} (D^t_i)\,dD^t_i - pD^t_i \quad (2\text{-}3)$$

通过对 $u^t_i$ 关于 $Q^t_i$ 求导，可得，

$$\frac{u^t_i}{Q^t_i} (e p)-(e p s) F(D^t_i),$$

$$\frac{{}^2u^t_i}{Q^{t\,2}_i} -(e p s) f(D^t_i) 0. \quad (2\text{-}4)$$

其中， $F(D^t_i)$ 是 $D^t_i$ 的累积概率分布函数。通过上面的分析我们可以知道，由上分析可知， $u^t_i$ 为凹函数，这表明其具有最大值。我们对其进行一阶最优条件求解，表明其存在最大值。因此通过一阶最优条件可得，

$$Q^{t^*}_i \quad F^{-1}\left(\frac{e p}{e p s}\right). \quad (2\text{-}5)$$

由于 $F(D^t_i)$ 的单调性，易得，

$$\begin{aligned} &Q^{t*}_i \quad e, \\ &Q^{t*}_i \quad 1/s, \\ &Q^{t*}_i \quad p. \end{aligned} \quad (2\text{-}6)$$

为了实现最大的本地云效益，有关假名分发的集 合为了最大化所有本地云的效益，最优的假名分发集合 $Q^*_t=\{Q^{t*}_1, Q^{t*}_2,..Q^{t*}_m\}$ 可以按照下面的公式得出，可通过下式求解，

$$Q_t^* \quad \arg\max_{Q_i^t}\left(\sum_{i\ 1}^{m} u_i^t\right),$$
$$st \sum_{i\ 1}^{m} Q_i^t \quad x\ T. \tag{2-7}$$

由分析可知，当且仅当满足 $\sum_{i\ 1}^{m} Q_i^t \quad T$ 时， $Q^*{}_t=\{Q_1^{t*}, Q_2^{t*},..Q_m^{t*}\}$ 存在。 如果不满足这个条件，假名的分发问 题也会受到 $\sum_{i\ 1}^{m} Q_i^t \quad T$ 的影响。通过以上的分析我们知道，假名的分发问题实质上就是， NP-hard 问题因此我们在对上式（ 2-7）处理过程中，运用遗传算法加以计算 [１９７]。有关具体算法流程图的介绍，详见图 2-5。这种方法需要用到以下几个步骤，首先我们需要对数据进行初始化、选择、对数据进 行交叉组合、并对数据进行便衣处理。其中，我们需要输入以下参数，具体有种群的大小，我们用 m 来表示，终止代数，我们用 G 来表示，个体算子，我们用 N 来表示，除此之外还有 交叉概率（ $P_c$）和变异概率（ $P_m$）。

## 3.3 仿真分析

在本小节，为了更好地预测方案的性能， 我们进行了仿真测试。考虑在面积为 25 平方千米的观察区域中安装四个本地云，记录为 $LC_1$，$LC_2$，$LC_3$,$LC_4$。我们对本地云中假名请求过程进行相应的分析，最后发现，这一请求呈现柏松分布的特点。以上四个本地云，平均每一分钟，可以发出的假名请求分别达到 50 次， 100 次， 150 次，两百次，并将其存储至列表中。在参数的设置方面，将 c 设置为 1，将 s 设置为 0.1，将皮衣设置为 0.3。对于中心云而言， 其每一分钟大约能够产生 600 个假名。为了研究分发假名系统的功能，我们对所提方案，进行了分析，而且还与典型的假名方案进行了对比。

图 2-6 对比在不同假名方案中的本地云获取的效益。由图可知，对于每个本地云来说， 对比根据需要进行假名的分配这种方案，我们发现均分的方案会产生更高的效益。。例如， $CL_4$ 在根据需要进行假名的分发方案中，比均分方案，产生的效益会高出约 44.44%。而对于其他的本地云盘而言，根据需求进行假名分发的方案，产生的效益也会更高，比另一种方案会高出 18.3%。其主要的原因是因为，在这种方案中，假名可以根据实际情况进行假名的分发工作。然而在均分方案中，出现了假名分配不均等的现象， $LC_1$ 和 $LC_2$ 会产生多余的假名，然而 $LC_4$ 却没有足够的假名 ，从而拉低了平均效益。在图 2-7 中，说明了系统参数对假名请求数量的最优选择有重大的作用。通过上图我们可以知道，我们可以增加 e 参数以及 p 参数的大小，减小 s 参数，可以帮助我们获得最优的假名需求量。

## 3.4 本章小结

在本章中，我们主要致力于假名的管理工作。并提出了三层假名管理系统，分析比对后，给出了一个最优的分发方案。为了提高假名的利用率，我们还借鉴了报童模型，求解出最优的假名请求数量。并通过仿真测试，我们发现假名的利用率更高，而且收益也提高了 。

# 第 4 章 基于雾计算的车联网位置隐私保护

在以前一章中，我们主要解决了假名的分发管理工作，完成这一工作之后，本章主要研究雾计算， 这一计算技术是现阶段比较流行的云计算延伸技术， 我们通过分析这种计算方法性质， 具体包括如下几个方面， 这种方法具有低时延、 覆盖面大、具有准确的位置感应功能等特点， 正是由于以上这些特点， 不断地简化了假名的管理工作。 传统的假名管理方式， 暴露出越来越多的问题， 具体来说主要有，成本较大并且具有比较大的延迟， 因此我们可以通过利用雾计算， 对管理方案进行完善。 在本方案的设计中， 我们将假名管理工作交给假明雾来负责。 进行仿真测试后， 我们发现这种方， 能够保证车辆通信过程中， 不受其他因素的干扰，安全性能较好，并且也更加经济，提高了假名管理的效率，除此之外，还对车辆的隐私进行了加密处理。

## 4.1 背景介绍

伴随着通信技术的不断发展， RNG 也在不断进步，对车进行联网处理也展现出了许多优势，具体来说，保障了交通运行过程的安全，除此之外，还促进了智能交通系统的不断完善［９８］ 。由于在本系统的具体应行中，根据硬件的需要，传统的车辆并不具备条件支撑车载技术的运用， 具体来说， 还应该提高其计算能力以及存储能力。 现阶段在车联网领域。 也不断地融入了移动云计算， 应逐渐的形成了现代车联网场景［９９］ 。

现阶段随着智能工具的不断普及， 移动业务所产生的数据流量与日俱增， 在车辆的通信方面，也产生了啊巨大的开销成本，传输时延问题比较严重［１（）（）］。除此之外，由于远端云的决策，离车辆的距离较远，因此这种鱼联网并不具备感知上下秦晋的能力。 通过上文的研究， 我们知道本章雾计算的研究主要目的是希望能够， 不断完善车联网的性能。 作为云计算延伸， 务计算也表现出了以下几个特点，支持本地化的决策，通信速度快。现阶段随着技术的不断发展，也有人在云在网络中融入了雾计算功能，增强了车联网的性能［１Ｑ１］ 。

在本章中，我们首先分析了线程技术，探究并不断融合了云计算与车联网，在这个过程中我们还提出了车联网范式。 在 F-IoV 中，到处都是具有低质量的通信资源、计算资源。可以借助无线通信网络，不断改善车辆内的通信网络质量，

提高网络的速度、 网络的稳定性、 以及网络的安全性 。我们将这些通讯资源部署在车辆附近， 这样一来车辆就能够快速的获取周边信息， 提高车载感知能力， 进而不断的提升服务体验。 除此之外， 我们应用本地化的数据处理技术， 不仅节省了网络的宽带，而且还能降低能耗。与此同时，也带来了一些问题。具体来说主要有，引入物计算功能的车联网在发展的过程中， 还是面临着一系列的你是泄露问题。

为了保证驾驶过程的安全性， 车辆还应该在规定的时间内， 向周边的车辆传递有关本车辆的身份信息 [1 6]，本车辆正处的地理位置，本车辆运行速度等一系列参数信息。 对这些信息的传送能够产生以下好处， 能够不断地加强车辆与周边车辆的交流，让驾驶员更了解周 边的状况，保证行车安全。但与此同时，这种信息的传递也会带来一些， 特别是会暴露该车辆的位置信息｜８７１。 更为了更好的克服这些缺点， 我们可以用假名来代替， 车辆在信息传递过程中身份信息 ［４８１。为了防止被恶意追踪，车辆可以随时变更假名。但是，随着现代车辆越来越多，假名管理工作也越来越复杂 ，车联网范式越发不能胜任假名管理的工作。为了改善假名管理工作，我们运用了雾计算，将假名管理的地理位置进行变更，最终转移至网络边缘进行处理。 我们可以采用分散化的管理方式， 即将假名部署在车辆附近， 从而网络边缘负责生成假名， 负责讲明的分发工作， 负责假名的撤销工作，这是一种全新的管理方式， 简化车联网范式的管理。 负责部署假名的本地认证中心，离车辆很近，借助于这一地理位置的优势，能够快速发放假名。除此之外，为了保护车辆的位置信息， 车辆还可以随时随地自行选择是否进行假名的更换，一般而言，车辆作出这一决定的主要依据是，依靠热点处，同时更换假名的车辆数目［４６］。

在车联范式中， 本地认证中心能够很快的获得同时进行假名更换的车辆数目，并且借助这一信息来帮助车辆进行假名的更换。 在本章中， 我们提出了车联范式的保护假名方案，除此之外，我们还运用了假名管理物技术。具体而言，将这些假名雾布置在各个地区， 分别负责所属地过往车辆的假名管理工作。 假名雾分布在各个地区， 是在务计算基础设施的基础上进行组合而成的。 对于每一个假名物而言，他们都对应着一个本地认证中心。 该本地认证中心主要是提供了同一热点处进行更换假名的车辆数目信息， 车辆便通过其感知功能， 选择是否进行假名的更换。由于车辆在发送信息的过程中， 并不想位置信息被泄露， 因此车辆可能需要多个假名进行及时更换， 因此也需要定期进行申请。 有关车辆如何获得新假名主要有以下几种方法 ：

（1）一次性请求法。我 们通过阅读大量的文献［８８］ ，我们发现车辆平均每年申请的假名数目可以达到 48830 个，申请后的假名存放在车辆中， 并且匿名

保存。因此假名储存的数目也对车辆内存提出了相应的要求。 如果系统查到恶意车辆的奥假名信息， 发出撤销指令， 这个时候， 系统发布这些假名的信息时间成本较大，也会增加不必要的信息［1 （） 4］ 。

（2）多次少量申请假名。通过这种方法申请的假名主要是来源于远程数据中心。当车辆需要隐藏自身的地理位置信息时， 便需要进行假名的申请， 此时车辆重复以上步骤［４８１。但是由于车辆与这些远程数据中心进行通讯的过程中，会消耗许多流量，产生很大的开销费用１１Ｇ５］ ，因此这种申请方式并不经济，也不利于环保。 综上所述， 我们需要设计出具有以下功能的假名管理系统， 具有上下文感知能力的， 可以根据自身所需要的假名数量产生相应的假名， 时延较低，效率高。

## 4.2 基于雾计算的假名管理框架

### 4.2.1 假名管理分层框架简介

图 3-1 展示了 F-IoV 中层次化假名管理的分层体系架构。 第一部分是云层系统，第二部分是雾层系统，第三部分是用户成系统。在第三部分中，车辆主要是借助车辆通信技术来传递信息，完成指令，连接雾计算设备，申请假名。在第二部分，务计算设备，安放在网络的边缘处，通过这种部署结构，给车辆提供一个增值服务，这种增值服务与云计算服务相类似。务计算设备可以通过多种方式，与其他实体的信息传递，主要的方式包括，有线方式，无线方式。五层中存在着大量的雾计算设备节点，在某一特定的地区内，他们能够整合在一起变成一个假名雾。个个假名雾负责假名管理工作，并根据指示将假名分配给周围的车辆，帮助车辆隐藏地理位置信息。云层中的云相对于雾层来说，展现出以下的优势，云层中的云内部能够实现大量的计算，并且存储空间比较大，因此在执行一些比较复杂的工作时更有效率。

### 4.2.2 假名管理分层框架模型

（1）云层： 在车联网范式全局认证中心，设置了管理假名的权限， 一般情况下， 智能交通部门充当这一部分。 这一全局认证中心， 内部配有一些具有防篡改作用的硬件， 并被布置在远程云中， 他们主要是利用云资源来实现对攻击的抵抗。从这方面而言， 这些节点非常可靠 ［４８］［1 （） 7］。当车辆准备出发时，应该在全局认证中心填写相应的信息， 这一信息可以用来作为识别的标志。 当车辆完成注册后，便会收获到车辆的公钥、车辆的私钥 、以及车辆的数字证书。与此同时， 车辆的注册信息还被从放在远程云数据库中。 车辆的初始钥密参数， 主

要由全局认证中心来管理，具体的参数见图 3-2 所示。在数据储存数据库中，存储了车辆使用过的或者正在申请的所有的假名信息。除此之外，在远程云端中，还设置了一个数据库， 名为事件数据库， 这一数据库主要是负责记录车联网范式中, 发生的一些非常规事件， 对这些事件进行记录， 以方便后期的调查以及处理。

（2）雾层： 在车联网范式中，一些网络基础设施，举例来说，有基站、路侧单元等，他们主要布置在网络的边缘处， 将它们连接在一起， 便形成了假名雾。除此之外， 在这些设施中， 还设置了专门的本地务服务器， 这些服务器连接互联网的方式选择比较多， 但是大多采用的是有线连接， 并且还提供了一个无线接口，旨在帮助车辆随时访问计算以及内部的资源。 实际计算应用的虚拟机主要是由本地务服务器来完成。 在雾层中， 每个假名物主要由以下几个部分构成， 第一部分是假名池， 第二部分是服务器设备， 第三部分是本地认证中心， 第四部分主要是负责记录违规事故的世界数据记录器。本地假名时，主要负责保存假名的工作。本地认证中心主要有以下几个部分构成， 第一部分是发行组件， 第二部分是服务组件，第三部分是撤销组件。 第一部分主要负责将新分配下来的假名分发给相应的车辆。第二部分主要是负责记录假名使用状况， 并记录在一个清单里。 后期我们可以借助这个清单， 实现假名与车辆的一一对应。 第四部分负责记录以及监督工作，具体而言主要包括， 负责对车辆行驶过程中的违规事件进行记录， 并且还加强对车辆附近的假名雾、 以及其他本地认证中心的监督管理， 并通过其内部逻辑，可以实现这两部分的相互督促，大大降低了工作量。在事件数据记录器中，还设置了一个黑名单， 这些黑名单主要是一些违规行为的车辆信息， 以便于后期的责任追究。 假名雾与其他实体的交流形式有两种， 第一种是通过有线方式， 第二种是通过无线方式完成。 为了检查假名的真实性， 车辆认证信息， 有本地认证中心传送至其他本地认证中心进行双重检验。

（3）用户层：在车联网中， 车辆内部配备了以下器件， 第一个是车载单元，第二个是全球定位系统， 第三个是假名存储单元， 第四个是无线通讯设备。 其中假名存储单元，主要储存 分发下来的假名，以及对应车辆的公钥、私钥。对系统而言，在系统中，其社交热点不止一个，在某一个具体的时间段，许多车辆会同时过往这一地点。 过往的车辆一般都会在这个社交热点进新家名变更， 因此一般也可以将这一地点称作为假名混合区［８７］ ［３９］。在这些地点中，有些打算更换假名的车辆，还可能展开博弈，来选择是否更换假名。一般来说，车辆最终决定主要依据在热点地区内进行假名更换的车辆总数。 在这一车联网范式中， 有关信息收集工作主要由本地认证中心来完成， 然后将这些信息传递给该地点的其他车辆，从而各个车辆来选择是否进行假名更换。 因此只要 该地点的其他车辆请变更假名的数量没有太大的变化时，一般决策也没有太大的变动。

### 4.2.3 假名管理分层框架优势

在我们的方案中， 我们将假名管理工作转移到网络边缘去执行， 分摊了管理的工作负荷， 交给其他假名雾共同完成。 为了隐藏车辆的地理位置信息， 我们主要借助车辆周围的本地认证中心来完成这一功能， 由于这些认证中心布置在车辆的周围，因此反应 较快，效率较高，能够很快的将假名分配给对应的车辆 ［1＜）１１。文献［１００］通过实验测试表明， 与中心云相比， 边缘数据中心延时低，能耗低。除此之外，本地认证中心负责，统计在热点区域申请假名的车辆数目，并将这些数目收集起来， 方便车辆作出是否更改假名的决定。 关于这种方案的主要优点如下：

（1）减少管理开销： 在车联网范式网络中，假名雾布置在各个不同的地理位置，分散了管理的工作负荷。 并且借助假假名雾来实现车辆地理位置信息的隐藏。因此地理位置上的优势，使得通信质量较好、速度较快。在本方案的假名管理，减少了流量的消耗，降低了开销费用。 实时的假名分发： 在各个不同的位置布置本地认证中心， 负责新假名的分发工作， 大大提高了工作的效率。 在假名的生成过程以及假名的分发过程中， 都隐藏了车辆的位置信息， 保护了车辆的隐私。采用这种方式有以下的优点， 可以有效的舒缓网络繁忙现象的持续时间， 可以分散申请假名的时间。 假名的请求工作主要是由本地认证中心来完成， 这样的工作安排，可以大大的减少了申请假名到分发假名的时间 。

（2）上下文情景感知的假名更换： 本地认证中心主要负责收集在社交热点中，申请假名的车辆总数， 并将这些信息储存起来。 其他车辆可以接收到这个信息，并据此来选择是否进行假名更换。 正是收到本地认证中心帮助， 大大提高了假名更换的参与率，也对车辆的地理位置信息进行了保护。

## 4.3 位置隐私保护的假名方案

### 4.3.1 假名方案介绍

有关位置隐私保护的假名方案，在我们看来，假名雾本地化管理被运用到各个本地认证中心的工作中，来处理假名的分发事物。本地认证中心其实是由不同的服务组件组成，服务组件可以生成假名服务列表，来方便车辆的假名管理工作。这些列表并不会定期上传到注册数据库中，因此也不会最终形成全球跟踪表。在车联网范式中，车辆申请假名后，由本地认证中心负责假名的分发工作，如果车辆获得公钥以及私钥、身份信息以后，地理位置发生了变化，但并不会变更负责发放假名的本地认证中心，除非车辆转而又其他认证中心请求假名。根据以上介绍，我们可以发现，为了提升服务体验，应该加强这两个认

证中心之间的交流 。

哥哥本地认证中心在管理假名的过程中，主要表现出以下几种优势 :第一，每辆车的身份信息会记录在一个本地认证中心，这种关系是一一对应的，采用这样的方式能减少隐私泄露的风险。第二，如果车辆在运行的过程中发生了故障，这一信息很快就会传送到本地认证中心，方便该中心及时取消其假名。这样可以大 大减少撤销的时间。第三，我们假设，绝大部分的车辆一般都在一个城市行驶［1 （） 9］ 。各个认证中心之间的交流，主要是借助网络来完成，这样的方式可以大大提高传输的速度 。

车辆自己的假名 $\{PID_i^k\}_{k=1}^w$ 会定期的宣传一些安全信息，以加强驾驶人员的安全意识。如 果 $v_i$ 假名并不够用到时候，可以向周围本地认证中心申请假名。完成以上步骤之后，本地认证中心未向车辆发放假名，车辆可以根据自己的需求进行更换。当 $v_i$ 离开当地，到达一个新的城市的时候，现在持有的假名是在以前的地方获得的，为了使用的衔接性，我们可以促进多个认证中心之间的交流，不断提高信息传递的有效性。如果 k 用完完内部储存的全部假名， $v_i$ 需要发出新的请求。为了实现我们所提出的方案，我们还提出了 2 种具体的机制。如表 3－1 是本次方案所运用到的符号。

（1）假名机制：在本章的设计中，我们假设 v 需要的假名数目为 w 个。假名数量的选择与具体的行程计划有关系。 ［8 9］［8 8］。更好地开展假名更换工作，可以带来极大的好好处，具体来说，可以隐藏车辆的地 理位置信息，防止被追踪。在一些社交热点中， v 可以根据当时车辆申请假名的数量，来决定是否更换假名。一般来说，当车辆驾驶在 2 个社交热点中间时，更换假名的时间间隔一般都是有规律的。

（2）加密和认证： 为了保证在无线通信的过程中信息的完整性，并及时的发现一些有违规行为的车辆，在本方案的设计中，我们特别增加了一些加密处理。当地认证中心会给每一辆车发送公钥、私钥以及相应的身份证书，一共有三套。公钥的主要作用是标识真实存在的身份，吃药的主要作用是，负责信息的传递，实现信息共享功能。证书的主要作用是，提供相应的感知功能。 具体而言， $\{PK_i, SK_i, Cert_i\}$ 用于车辆到基础设施的通信，而不是使用车辆的真实身份， $\{PID_i^k, SK_{PID_i^k}, Cert_{PID_i^k}\}$ 用于车辆广播安全 “ 心跳 ” 信息时保护其真实身份， $\{GID_c, SK_{GID_c}, Cert_{GID_c}\}$ 主要在车辆更换假名之前用于发送假名更换请求和回复。

### 4.3.2 检测分析

（1）系统初始化和密钥生成： 为了使系 统回到原来的状态，并完成生成秘

钥的工作，我们所主要采用的方案名为 Boneh－Boyen 短签名方案。当车辆 $v_i$ 第一次加入车联网时候， 我们能通过远程云端， 来捕获该车辆的一些信息， 具体包括，该车辆获得的公钥、私钥，身份证书。我们用 $PK_i$，来代表公钥，用 $SK_i$ 来代表私钥，我们用 $Cert_i$ 代表身份证书。一般来说，认证中心实现洗衣信息共享功能的时候， 优先将信息传递到离 $v_i$ 绞较近 的假名雾（例如 $LC_j$）将一组 w 个假名 $\{PID^k_i\}^w_{k=1}$ 分配给 $v_i$。这些假名附有相应的公钥／私钥和证书，即全局认证中心在事件数据库中生成一个跟踪表 $ID_i$，$PK_i$，$Cert_i$，$LC_j$，$\{PID^k_i\}^w_{k=1}$。在这之后，全局认证中心还会借助公钥， 来完成工作， 将$\{PK_i$，$Cert_i$，$LC_j$，$\{PID^k_i\}^w_{k=1}\}$ 这个集合，所表示的跟踪信息发送到其他的基础设备中。 在本章的介绍中， 我们假设所有的路测单元运行可靠 １１１（＞１１１１１１。 并且关联度比较大， 这样更能方便技术设备之间的交流。

（2）假名管理的基本操作： 当 $v_i$ 在当地道路上行驶的时候，一般来说，他们利用假名来进行信息共享的次数一般都有规律。一般间隔为 300ms［３９］。之所以要频繁的更换假名， 主要还是为了隐藏位置信息。 除此之外， 为了保证信息发送以及接收过程的顺畅、可靠，与此同时， $v_i$ 需要在共享信息上签名，并写上具体的时间，通过这种方法来提高消息的可靠性。 ［８７］。$v_i$ 接收到周边车辆的共享信息时， 可以根据共享信息上的内容， 来判断该消 息是否真实。 当车辆假名即将用完的 时候， $v_i$ 还应该及 时的发送假名申请。

（3）本地假名请求： 在用完所有假名之前， $v_i$ 必须必须在当地， 重新申请假名，来隐藏地理位置信息，防止被他人恶意追踪。请求新的假名以保护隐私。 $v_i$ 发送把假名请求加密后发送到本地认证中心 （$LA_j$），这个假名请求包含请求的假名数量，当前所处的地理位置，正在使用的 $PID^n_i$、$Cert_i$、$Cert_{PID^k_i}$。$LA_j$ 验证 $v_i$ 的信息的合法性。 如果 $v_i$ 处于 $LA_j$ 的通信覆盖范围内并且是其身份合法， 则 $LA_j$ 将发送一组新的假名集合 $\{PID^k_i\}$给车辆。当 $v_i$ 对假名的一系列信息进行核查之后，便把这些假名放在列表中进行存放，存放完之后，将信息发送到 $LA_j$。完成以上工作之后， $LA_j$ 会对该信息进行不断的更新，这些信息主要包括，车辆 ID、车辆发出的假名申请、以及申请假名的数量 等最终这些信息会被全局认证中心所接收，车辆 $v_i$ 的更新信息，将 会存放在跟踪表里。

（4）本地假名更改： 如果发生以 下情况， 正在使用假名 $PID^k_i$ 的车辆 $v_i$ 想要更换假名，它将发送加密信息给他会将经过加密处理过的信息传送到。 $LA_j$（如图 3-6 的协议 4 所示）。该消息的主要内容，不仅包括当前使用这个假名的相关消息，还包括下一个假名的相关消息。 $LA_j$ 接收到该消息之后，需要完成以下的工作，通过比对假名中的相关信息， 与共享网络中的签名， 来判断该假名的合法性。完成核查工作以后， 本地认证中心应该对该车辆的所属地进行更新， 并保存

到该车辆的服务记录里面。 $LA_j$ 还会将信息发送给车辆 $v_i$，保证假名更换的工作已经顺利完成。除此之外，$LA_j$ 还会将所有的本地车辆都填列到本地服务列表中，以方便车辆假名的管理。 而且，还会在 特定的时间间隔内， 将更新的列表发送给全局认证中心，用来更新记录违法行为的车辆 ID 的世界数据库，保证跟踪表是最新的。

（6）跨区域假名请求：如果 $v_i$ 使用 $LA_j$ 分发的倒数第一个假名已经到达另一个区域，（由 $LA_m$）进行心跳广播，若 $v_i$ 需要更换 假名，他会从新疆假名申请信息传递给 $LA_m$。发送假名请求的时候， 其传递的信息包括以下几个方面， 包括车辆正在使用的假名信息，以 及该车辆的真实信息。车辆申请假名可表示为 ：

$$request \quad E_{PK_{LA_m}}(Pseu\_req \| PK_i \| Cert_i \| PID_i^{w-1} \| Cert_{PID_i^{w-1}} \| TS)。$$

$LA_m$ 负责检验就假名的信息、 签名有效性、 证书的合法性。 验证旧假名及其签名、证书的有效性。 此后，$LA_m$ 与 $LA_j$ 进行通信， 通知 $LA_j$ 完成以下操作 :删减车辆 $v_i$ 中的记录，指令发送成功后，记录更新工作马上暂停。就在这个时候，$LA_m$ 开始记录有关车辆 $v_i$ 的一些身份信息 ，并分配一组假名给这些车辆。分配过程具体实施，与申请本地假名的具体操作没有太大的区别。

（7）跨区域假名更换： 当 $v_i$ 在以下这种环境中工作时，被 $LA_m$ 覆盖。这个时候，如果车辆 $v_i$ 想更换假名， 应该从新发送跨界的假名更换信息。具体的操作与本地更换没有什么太大的差别。当 $LA_m$ 接收到车辆 $v_i$ 的更换请求后，应该及时检验，车辆 $v_i$ 身份的合法性。通过验证信息， $LA_m$ 确认 $v_i$ 是由管理的车辆 $LA_j$ 将更新关于 $v_i$ 的假名更换记录，

（8）假名撤销： 在本次方案的设计中，我们实现的任何监控范围是非常广的，能够对一些违规车辆的行为进行实时的监控， 而且这些监控工作主要是由周边车辆以及雾计算等设施设备来完成的。 举例来说明， 如果某一车辆， 进行假名更换，并且在行驶过程中出现了违规行为，此时 vi 会马上注意到，并将这些行为记录到数据库中， 完成备案工作， 然后提交报告给周围的本地认证中心。 报告中主要记录有， 该车辆发生违规行为的证据， 触犯的交通条例， 举报该车辆正在使用的假名证书，并且通过信息传递通知周围的车辆。 具体形式如下

$$Report \quad E_{PK_{LA_j}}(Tvpe \| Cert_{PID_k} \| Cert_{PID_i} \| Sign_{SK_{PID_i}}(Tvpe \| Cert_{PID_k} \| Cert_{PID_i} \| TS) \| TS)。$$

接收到报告之后 ，$LA_j$ 还将进行以下工作，核查该报告的真实性，以及车辆身份的合法性，完成核查工作之后，需要将这个报告存放在事件数据记录器中。最后将信息传递给全局认证中心， 进行二次检验， 通过搜索跟踪表， 对该车辆 vi key 的真实身份进行核查，并将核查结果公布。如果在检验的过程中，证实了该车辆 vk 确实有发生过违规行为，那么全局认证中心便会自动的将车辆身份信息填列到黑名单中，并将更新的黑名单通过信息共享功能告知所有的车辆。

## 4.4 本章小节

本章首先详细介绍了车联网隐私保护的背景， 然后我们提出了， 融入了雾计算功能的假名管理方法。 对其进行介绍分析， 系统生成密钥之后， 将假名分发给附近车辆。