车辆自组网的位置隐私保护技术研究

张建明[1]，赵玉娟[1]，江浩斌[2]，贾雪丹[1]，王良民[1,2]
(1. 江苏大学 计算机科学与通信工程学院，江苏 镇江 212013；2. 江苏大学 汽车工程研究院，江苏 镇江 212013)

摘 要：车辆自组网的位置服务在解决道路安全问题、为驾乘者提供便捷服务的同时，也带来了相应的隐私保护问题。总结了隐私保护内容，重点分析了车辆自组网的假名和签名 2 类隐私保护技术，其中假名方案分为基于特殊地形、基于安静时段、加密 mix-zones 和 mix-zones 通信代理；签名方案分为群签名和环签名。继而针对隐私保护水平的高低，分析了匿名集合、熵度量、数学理论分析和形式化证明几类主要的位置隐私度量方法，对其各自的特点进行了总结比较。

关键词：位置隐私；隐私保护；车辆自组网；基于位置的服务
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2012)08-0180-10

Research on protection technology for location privacy in VANET

ZHANG Jian-ming[1], ZHAO Yu-juan[1], JIANG Hao-bin[2], JIA Xue-dan[1], WANG Liang-min[1,2]
(1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;
2. Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China)

Abstract: Location-based services in VANET solved the problem of road safety, and provided the convenient services to drivers and passengers. But it also brought new problems of privacy protection. The content of privacy protection was analyzed, and put emphasis on two kinds of privacy protection technology based on pseudonyms and signature respectively. Pseudonym-based schemes were classified as special-area based, silence-period, cryptographic mix-zones and mix-zones communication proxy based schemes. Signature-based schemes were also divided into two classes: group-signature and ring-signature. The evaluation methods for privacy protection level were surveyed, in which anonymity set, entropy metric, mathematical analysis theory and formal analysis were discussed and compared.

Key words: location privacy; privacy protection; vehicle ad hoc network; location-based service

1 引言

车辆自组网(VANET, vehicle ad hoc network)是一类在交通领域有广泛应用的移动自组织网络，它支持动态、随机、多跳拓扑结构。车辆自组网通信范围内的车辆可以自组织地连接成一个移动的网络，相互交换各自的车速、位置等信息和车载传感器感知的数据，可使驾驶者在超视距范围内获得实时的路况信息和其他车辆的行车信息，从而解决道路交通安全问题，提高行车服务质量。

典型的车辆自组网由 3 部分构成：车辆子网、网络运营商和服务基础设施部分。其中，车辆子网是由车载通信单元(OBU, on-board unit)连接而成的自组织网络；网络运营商是已有的基于 Internet 的有线无线网络设施；服务基础设施包含认证中心(TA, trusted authority)、服务供应者(SP, service

收稿日期：2012-02-20；**修回日期**：2012-05-18
基金项目：国家自然科学基金资助项目（51108209）；江苏省自然科学基金资助项目（BK2011464）
Foundation Items: The National Natural Science Foundation of China (51108209); The Natural Science Foundation of Jiangsu Province (BK2011464)

provider)和路边单元(RSU, road-side unit)。为此车辆自组网的通信也分为 2 个部分：车与车(V2V, vehicle to vehicle)通信和车与基础设施(V2I, vehicle to infrastructure)通信，如图 1 所示。

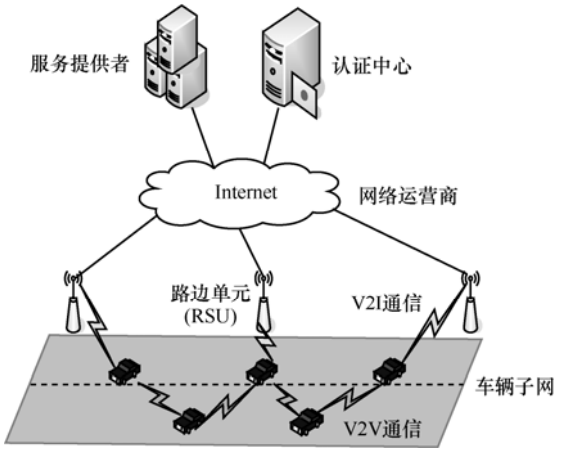


图 1　典型的车辆自组网结构

车辆网络所接受的是一种位置服务(LBS, location-based service)，LBS 提供的服务与用户提出请求的位置有关[1]。例如，V2V 中，车辆要实时广播自己的位置、速度信息给周边车辆，以防止相互碰撞；V2I 中，车辆基于位置来向 RSU 请求服务，服务提供者则基于位置信息，通过路边单元给车辆提供各类增值服务。显然，使用 LBS 容易造成位置隐私的泄漏[2]。就 VANET 的应用与网络结构来说，至少有 3 类位置隐私泄露方式[3]：路边单元或位置服务器中用户信息的泄密的直接方式；通过观察被攻击者行为获取位置信息观察方式；通过与车辆位置的通信连接来确定用户位置追溯方式。

然而，VANET 中车辆信息、驾乘人员及位置信息往往捆绑在一起的，驾乘人员在享受基于位置服务的过程中，有强烈的隐私保护需求——不愿意泄露自己的身份、现在或将来的位置等重要信息。多数驾乘者是无法接受在服务的同时遭受个人隐私泄露。为此，要推广和应用 VANET 以及基于 VANET 的位置服务，必须解决好车辆使用者的位置隐私保护问题。

本文主要综述了国内外近几年来针对车辆自组网的位置隐私保护方法及相关技术的研究，在介绍各类方法基本思想的基础上，对其主要特点进行了归纳总结，并指出了还需要重点解决的问题。本文的组织结构如下：首先，简单介绍车辆自组网的组成和特点以及网络中的隐私保护内容；接下来，对现有的隐私保护技术进行总结比较，分析各方案的基本思想、适用环境及优缺点；继而对各种隐私度量方案进行分析；最后，总结全文并提出车辆自组网中关于隐私保护的进一步研究内容。

2　车辆自组网的隐私保护内容

当前，有关车辆自组网隐私保护技术的研究，多数和安全研究相关，而实际上，隐私和安全是相关而并不相同的 2 个概念。安全是指网络不受外界威胁和攻击，文献[4]认为 VANET 内的位置安全主要有 3 个要素：保密性(confidentiality)、完整性(integrity)和可用性(availability)，而文献[5]扩充了这个范围，指出 VANET 内的安全需求主要包括：身份验证(Authentication)、保密性(confidentiality)、隐私(privacy)和付费(billing)。这个广义的安全范围，不仅指出受威胁的目标不单指车辆，也可以是 SP(服务提供者)；还包含了隐私，隐私是不愿意被别人知晓的信息。

车辆自组网内的隐私通常包含身份隐私、服务隐私和车辆位置隐私 3 个方面。身份隐私，即网络内车辆及车辆用户的真实身份，包括驾驶证号、姓名、身份证及账户号等关键信息，需要车辆频繁变换身份标识，防止攻击者关联前后的标识，又称为句法隐私。服务隐私即某车辆在享受一个 LBS 的过程中达到的身份、服务信息和位置隐私。服务信息隐私包括内容隐私、前向隐私和后向隐私 3 个部分：内容隐私，即车辆在要求服务时的服务内容，如艾滋病医院、假发维护等；前向隐私是指某辆车在得到一个 LBS 的认证授权前，不能从 RSU 或别的车辆那儿获取由此 LBS 发布的任何服务内容；后向隐私，即某车辆在离开一个 LBS 后，不再具有继续享受该服务未来内容的权利。身份隐私和服务隐私均可通过现有的隐私保护技术移植得到实现。

位置隐私是车辆自组网隐私保护中的关键难点，一方面，位置服务中所有的服务都是基于位置信息提供的，在某辆车进入某位置前或离开后，就不能获得服务的内容；另一方面，位置信息本身是用户隐私的重要部分，不能泄露。位置隐私不仅需要保护车辆的物理方位和路径轨迹不泄露，还需要防止攻击者利用中心消息中的位置、速度等信息重构车辆的轨迹，有时候也称为语义隐私。位置隐私可能以“通过通信连接重建用户位置信息”的方式泄露，所以位置隐私保护也应包含通信隐私。通信

隐私是指通信过程中通信双方的身份和位置信息以及通信内容不被泄漏或各自的身份与位置不被关联。通信隐私包括 V2V 通信隐私和 V2I 通信隐私 2 类。

3 位置隐私保护技术

目前，国内外针对车辆自组网隐私保护技术的研究很多，提出了一些实用性的隐私保护技术，其本质都是隐藏车辆的真实身份和通信中使用的身份之间的一一映射关系，以实现车辆匿名、隐藏车辆或者车辆身份模糊等。最常见的方式是在指定区间让车辆更换假名的 mix-zone 假名方案和将单个车辆看成一个群体中一员的群(环)签名方案，这些隐私保护技术都结合了密码学方法。

3.1 基于 mix-zone 的假名方案

基于 mix-zone 的假名方案的基本思想是：为车辆配备大量不揭示其真实身份的假名(pseudonyms)，每个假名仅使用一段时间后进行更换，而更换假名的操作是在特定的地理区域(mix-zone)内进行的。假名(pseudonyms)是随时间(或速度)而改变的短暂身份标识。使用假名可以保护车辆的真实身份，但是如果长时间使用同一假名相当于未使用，故需要定期更换假名。假名方案[6]为防止连续跟踪，让车辆配有无关联的多个假名，通过某种机制阶段性地更换，达到隐私保护的目的。Capkun[7]给出了一个基于时间的假名定义，如式(1)所示。

$$P_{v_1}(t) = HMAC_{K_{V_1}^{-1}}(ID_{v_1}, t) \tag{1}$$

其中，P_{v_1} 是车辆 v_1 在 t 时刻产生的假名，HMAC (hash mutual authentication code)是一个密钥散列函数，ID_{v_1} 表示车辆 v_1 的真实身份，$K_{V_1}^{-1}$ 表示车辆 v_1 的私钥。不同于文献[7]中假名更新以时间为度量，文献[8]提出了以车辆速度决定假名更新的频率，从而避免了高速长距离假名不变带来的跨 RSU 的位置隐私泄露。假名更换常和路径混淆[9]、随机加密[10]以达到更佳的效果，其中路径混淆是指假名在具有相似路径的节点间变换；随机加密结合了加密消息和加密阶段随机的思想。

Mix-zone 的概念首先由 Beresford[11]在 2003 年提出，是指假名变换的地理区域。Beresford[11]使用文献[12]中的通信 mix-zone 来处理移动节点的位置问题。Beresford[13]在 2004 年给出了基于位置服务的 mix-zone 模型架构，其考虑对象是行人；随后文献[14~16]也基于该模型讨论了移动节点在特定区域更新假名。其思想类似于混合网络中的混淆节点，通过变换消息的编码和顺序，达到难以关联消息发送者与接收者的目的[6,17]。在车辆自组网中，mix-zone 的选取与设计与混淆效果密切相关，目前常见的方式有基于特殊位置、基于安静时段、基于加密空间和基于通信代理等 4 种典型方式。

3.1.1 基于特殊位置的 mix-zone

基于特殊位置的 mix-zone 是指事先指定某个地理区域，在该区域更换假名，以达到车辆混淆和隐藏的目的。Buttyán 等[18]2007 年首次将 mix-zone 方法用于车载网络，其 mix-zone 模型如图 2 所示，其中，A、B、C 为车辆入口，D、E、F 为车辆出口，车辆在 mix-zone 中更换假名，选择不同路径离开，从而起到混淆的作用。

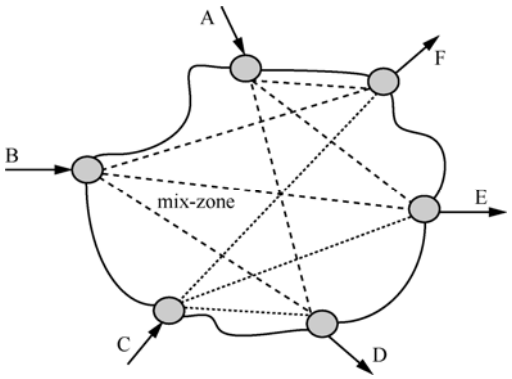


图 2 公路网中形成的 mix-zone

文献[18]将道路网络模型分为攻击者可观察和不可观察区域，在不可观察区域用 mix-zone 建模，车辆在穿越该区域时停止发送一些消息来更新假名、混淆身份。为扩展实际地理情形对 mix-zone 选取的限制，文献[19]构造了直线路面的 mix-zone。如图 3 所示，车辆 A 和 B 在进入 mix-zone 前后的消息标识发生变化，加大了跟踪的难度。但这种方法在车载网络密度较小的情况下，因为攻击可以通过信号跟踪，隐私保护效果并不明显。

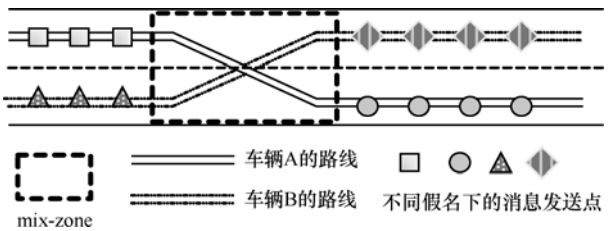


图 3 在直线路面上构造 mix-zone

文献[20]提出在有许多车辆聚集的交通红灯处、大型商场的免费停车场等社交点(social spot)建立 mix-zone 的思想。Lu 等[21]将文献[20]设计的匿名分析方法提炼为 PCS(pseudonym changing at social spot)策略，并用博弈论证明了它在实际中的可行性。

利用基于特殊位置的 mix-zone 方案，在某些特定的地理位置更换假名确实起到了一定的隐私保护作用。然而，总体来说，这种基于特殊地形、地点的 mix-zone 方法，很容易被基于地形的其他监控技术所攻击，从而失去其隐私保护的目的。

3.1.2 基于安静时段的 mix-zone

鉴于基于特殊位置方案的地理局限性，许多研究者采用基于安静时段的 mix-zone 方案。基于安静时段的 mix-zone 是采用分布式思想的动态 mix-zone，车辆自己或彼此之间形成一个安静时段，然后更换假名，从而实现在不需要特定交通基础设施的帮助下完成假名的更换过程。SLOW[22](silence at low speed)可在不与其他车辆和第三方设施的合作下创建自己的 mix-zone。其基本思想是：在车辆速度不下降到速度阈值(比如 30km/h)以下时，不给中心发送消息，车辆在这样的一个安静时间段内更换假名。

然而，安静时段的选取是困难的。SLOW[22]认为低速情况下碰撞事故少，即使发生也不会很严重，所以安静时段设置在低速时；文献[22]认为最理想的地方是城市交通信号灯处，车辆必须减速的地区、车道选择较多，事实上这结合了基于特殊位置 mix-zone 中地形和社交点的优点。此后，文献[23]提出假名在指定的时间段内进行假名更新；文献[24~26]指出由参与者决定何时停止所有通信更换假名，其中文献[24]则需要一个辅助节点之间协调它们的安静时段的中心机构；文献[25]充分利用群的概念，区内车辆通信实行匿名控制及拥有一个随机的安静时段，可减小单个目标车辆的位置跟踪；文献[26]中的节点独立决定是否在已形成的 mix-zone 中变换假名，但是基于博弈论(game theory)结果表明，自我的动态行为降低了节点间成功协调的机会。

总体说来，在车辆多的社交点完成假名更新是有一定危险系数的，而且车辆间关于安静时段的协调以及假名更换成功的概率都是需要重点考虑的问题；更为重要的是，结合使用基于位置假名更换的方式，拥有了其优点，也无法躲避其易于跟踪的缺点。

3.1.3 加密 mix-zone

基于特殊位置和安静时段的研究方案一般采取在 mix-zone 停止所有通信的方式，然而这在不同程度上造成了 VANET 安全性能损失。加密 mix-zone 方法是对某个地理区域加密，保证区域内的通信安全进行，而车辆在形成一个匿名群体通过 mix-zone 并更换假名后，攻击者将难以辨认出哪辆是他所要跟踪的。

文献[27,28]均采用了加密 mix-zone 中消息的方法代替停止所有通信。Freudiger 等[27]提出 CMIX(cryptographic mix-zone)协议，创建一个对称密钥 k，作为 mix-zone 的空间密钥。k 由 RSU 分配给进入 mix-zone 混合区域的合法车辆，mix-zone 内通信的信息都必须经过 k 的加密。CMIX 为加强效果，文中联合多个加密 mix-zone 形成 mix network(车辆混合网络)。其创建对称密钥的过程如下：

$$V \to RSU : sign_{K_V}(request, T_S), sign_{K_{CA}}(P_V, pub(K_V))$$

$$RSU \to V : E_{\mathrm{pub}(K_V)}(sign_{K_{\mathrm{RSU}}}(P_V, zk, T_S)),$$
$$sign_{K_{CA}}(P_{\mathrm{RSU}}, pub(K_{\mathrm{RSU}}))$$

$$V \to RSU : sign_{K_V}(ack, T_S), sign_{K_{CA}}(P_V, pub(K_V))$$

Dahl 等[28]在十字路口构造加密网络模型，如图 4 所示，采用 CMIX 协议[27]为车辆进入 mix-zone 分配密钥，并形式化分析了加密 mix-zone 的隐私模型。在分析实验结果的基础上，对 CMIX 协议进行了改进，即在 RSU 的公钥下加密请求和回复的消息。重建实验场景后，大多数理想模型中的隐私在 CMIX 模型中也能达到。

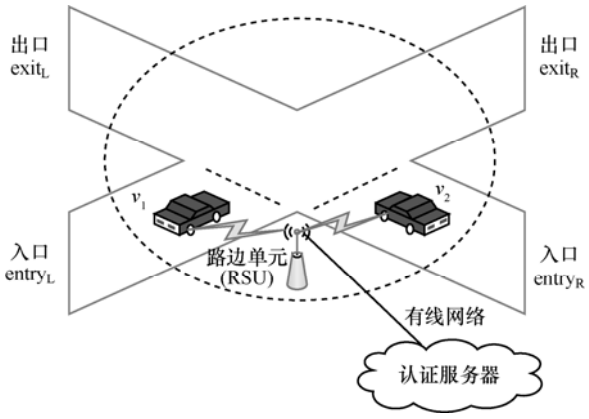


图 4　加密 mix-zone 十字路口模型

总体来说，加密 mix-zone 提高了消息隐私性与车辆不可跟踪性，但是同样，车辆假名更换成功仍需要足够的车辆数目；同时，加密也意味着更大的通信开销与延迟。

3.1.4 mix-zone 通信代理

为减少车辆身份及发送消息的泄漏，有学者提出在 mix-zone 内的通信采用第三方代理方式。Sampigethaya 等[29]在随机安静时段[23]的基础上，让车辆形成群体，每个群中的领导者代表群内所有成员利益，匿名与 RSU 通信，使每辆车获得 LBS 的应用。以群体隐藏了个体，达到匿名与隐私保护的效果。

ProMixZone 方案[30]是针对城市交叉口及高速分叉路口的更换假名并保证消息传送的有效方案。该方案中的车辆允许通过一个可信代理发送消息，每辆车在进入 PMZ(mix-zone with communication via proxy)前，会收到来自包含路边代理的公钥广播消息。车辆在需要发送消息时，先用自身私钥产生签名，然后用代理的公钥对签名后的消息进行加密，再发送给代理；代理汇总掌握 PMZ 内所有车辆的消息，在移除相应消息中的证书与签名后，代理用自己的私钥对消息进行签名，并用接收消息车辆的公钥加密后发送给对应车辆。

然而，代理方式虽然保证了消息的匿名传送，但由于它的任务繁重，也成为了整个过程的瓶颈。对于 mix-zone 的研究，还有学者[31]考虑了多个 mix-zone 在城市中的优化部署问题，并用有向图形式化了一个城市 mix-zone 分布。

3.2 基于签名的方案

数字签名依靠公钥加密技术保证了消息的完整性、发送者身份验证以及防止抵赖，从而提供了一个辨别消息合法性的方法。在基于签名的车辆位置隐私保护方法中，主要是基于群签名和环签名的方案，利用一个群体混淆群体内个体之间的区分，从而实现车辆匿名性的目的。

3.2.1 基于群签名的位置隐私方案

群签名方案的基本思想是，车辆先形成一个群体，群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样，群签名可以是公开验证的，而且可以只用单个群公钥来验证；不同的是，群签名保护签名者的匿名性，只有群管理者才可以跟踪签名者。为此，该方案可以用于车辆网络，一方面，实现匿名认证；另一方面，实现可信中心对特定车辆的跟踪。

最早的群签名方法由 Chaum 和 Heyst[32]提出，随后 Boneh 和 Shacham 提出了短群签名方案[33]和 VLR(verifier-local revocation)机制。但是 VLR 机制中签名撤消的消息只发送给签名认证者，而不发给签名者，导致已撤消的成员在撤消状态下仍然可以使用之前的群签名保持匿名性，使得该方案存在后向关联性。Nakanishi 和 Funabiki[34]提出了改进的 VLR 群签名方案(记为 NF05)，消除后向关联特性。而文献[35]提出了一个改进的 NF05 群签名方案并应用于车辆网络，获得一个拥有更短签名长度和更少计算开销的身份认证方案。改进 NF05[35]中有 2 种身份认证机制，需要服务的 OBU 发送签名给 RSU，RSU 查找群公钥和撤消列表，核实签名合法后允许 OBU 下载服务。随后，动态的隐私保护的密钥管理方案 DIKE[36]被提出，它是一个源于有效群签名的隐私保护身份验证机制，可避免用户可能对同一个 LBS 双重登记而导致的攻击(如 Sybil 攻击)，在达到用户的隐私保护的同时，还能防止车辆用户的双重登记。

GSB[37]综合采用群签名技术和身份签名技术，使得 OBU 不需要存储大量的匿名密钥，易于更新；而且可信中心可以有效地跟踪目标 OBU。然而，其 OBU 能够处理的密钥撤消列表比较短，在面对大规模的密钥撤消及紧迫的安全消息匿名认证时，该方案面对繁重的核实过程将不大可行。针对此问题，Lu 等[38]提出有效的条件隐私安全保护(ECPP[38]，efficient conditional privacy preservation)协议，该协议基于 HAB(huge anonymous keys based)和 GSB 协议，在满足可信中心一定程度跟踪的同时，有效地处理不断增长的撤消列表。ECPP 协议只保持所需匿名密钥的极小存储，同时在安全消息的快速认证上增加了容量和有效的条件隐私跟踪机制。此后，SPRING[39](social-based privacy-preserving packet forwarding)协议研究车辆延迟容忍网络中分组转发应用时接收者的位置隐私，它首次提出统计各交通叉路口 RSU 的密度；利用 RSU 的认证，达到分组的可信转发；并采用 ECPP 协议[38]的思想，使得可信中心可在一定程度上实现对 OBU 的跟踪。

3.2.2 基于环签名的位置隐私方案

群签名方案可以实现隐私保护，然而是建立在群管理者不会恶意揭露成员身份的基础上的。由于群签名方案中，成员身份(公钥信息)是由第三方保

管(群管理者)的，一旦该第三方被攻击者攻破，则可能会任意揭露成员身份。由此，有研究者在 1999 年提出使用环签名的方法保护隐私[40]。环签名(ring signature)是群签名的一个变种，环签名方案在无需群管理者的情况下，实现了绝对隐私保护。环签名允许签名者通过认证来确认消息可靠性，并且保证签名者在几个可能的签名者中无法辨别，从而实现匿名性。环签名允许车辆自由设立签名，即在车辆行驶过程中，无需考虑其他签名车辆就可以建立签名群发送消息。然而，这种绝对匿名情况下，匿名性可能被滥用。文献[41]提出了一个基于环签名的不可否认性机制，目的是在没有群管理者的情况下达到车辆的条件隐私。车辆自组织形成车群，采用公钥签名，该签名可以证明消息的准确性而无需揭示签名者的身份。

由于车辆的移动性，VANET 的网络拓扑结构是动态变化的。环签名方案可以满足由网络拓扑结构动态变化带来的通信要求。因为无需互相同意和消息交互，环成员可以快速变化，而且，小的环仍然可以确保签名者的匿名性。

3.3　混合方案

以上各种基于 mix-zone 的假名方案和群签名环签名方案各有其优势和不足，一个研究思路是结合不同方案，利用其优点相互弥补不足之处，获得具有更有效果的混合方案。混合方案由于综合使用了多种方法，在综合性能上具有更优的效果。

Spring[42]方案结合了假名和群身份思想，网络中的每辆车的假名均配有一组群的公钥和私钥，车辆用私钥签名消息，用假名进行通信。文献[27,28,30]中，将假名方案中结合了数字签名思想。AMOEBA[25]是最有代表性的混合方案，采用了 3 种方式来实现假名、群概念、数字签名的思想，如利用组建车辆的群导航提供匿名，随机安静时段提高目标车辆在导航中位置隐私，签名密钥管理实现安全与隐私的权衡，达到了减缓某辆车的位置跟踪的理想效果。

3.4　隐私保护方案比较

本文在介绍以上各类隐私保护方案的同时，对其各自的特点进行了分析。总体说来，各方案均有自身的优点，也存在一定的不足。本节的主要内容是在隐私保护内容、针对的攻击类型以及隐私保护性能 3 个主要方面，对以上典型方法进行综合比较。一般情况下，衡量隐私保护性能时主要使用 4 个要素：匿名性、无关联性、不可跟踪性和顽健性。其中，匿名性是指改变或隐藏车辆的身份，不用真实身份进行车辆自组网络内的通信；关联性是车辆的前后身份标识、前后位置以及身份标识与位置的关联，隐私保护需要剔除这种关联，实现上述参数的无关联；不可跟踪性指攻击者不可以利用多种方式达到跟踪车辆的目的，这些方式包含观察和关联前后位置、收集离散方位点等进行预测；而顽健性是指车载网络能够抵抗攻击者的强度。在此，只给出各方案的隐私保护性能的结果，具体的度量方法将在下一节作具体陈述分析。表 1 给出了比较结果。

表 1　　**位置隐私保护方法的比较**

位置隐私保护方法		位置隐私保护内容			攻击者类型			隐私保护性能		
		车辆身份	通信内容	轨迹	被动	主动	匿名性	无关联性	不可跟踪性	顽健性
mix-zone	特殊地形[18]	√	×	√	√	/	√	中	中	低
	安静时段[22]	√	×	√	√	/	√	中	中	低
	加密 mix-zone[27]	√	√	√	√	/	√	中	低	低
	通信代理[30]	√	√	√	√	/	√	高	中	中
路径混淆[9]		√	×	√	√	/	√	中	低	中
随机加密[10]		√	√	√	√	/	√	高	中	中
群签名	改进 NF05 方案[35](认证)	√	√	×	/	/	√	高	低	低
	GSIS 协议[37]	√	√	×	√	√	√	高	低	中
	ECPP 协议[38]	√	√	×	√	√	√	高	低	中
	环签名[41](认证)	√	√	×	/	/	√	高	低	低
	混合方案[25]	√	√	√	√	/	√	高	高	中

4 隐私保护水平的度量方法

表 1 中在描述隐私保护技术水平时使用的 4 个要素是目前度量隐私保护水平的主要指标，相关工作都围绕着这 4 个指标来讨论隐私保护技术的隐私保护能力。但是不同的度量方法在对各个指标的关注上是有所差异的，度量方法大致可以分为基于匿名集合度量、基于熵关联性度量、基于分布概率度量和顽健性形式化证明 4 类。

4.1 基于区域匿名集的度量

匿名集合的概念早在 1988 年就已被学者提出。一般指在某个攻击者控制的区域范围内，同步变换匿名证书的所有 OBU 集合。某区域的匿名集合越大，表明隐私程度越高。以文献[29]为例，某个目标的匿名集 S_A 表示让攻击者难以分辩出目标身份的假名集合，$|S_A|$表示集合大小，$v(A_r)$表示目标车辆所在范围 A 内车辆总数目，则 $v(A_r)$满足空间泊松分布，即满足式(2)。所以，一个目标匿名集合的期望大小可以表示为式(3)。

$$p_r\{v(A)=i\}=\frac{(\rho A)^i}{i!}\mathrm{e}^{-\rho A} \tag{2}$$

$$\begin{aligned}\mathrm{E}\{|S_A|\}&=\mathrm{E}\{v(A_r)\,|\,v(A_r)\geqslant 1\}\\&=\frac{\mathrm{E}\{v(A_r)\}}{1-P_r\{v(A_r)=0\}}=\frac{\rho A_r}{1-\mathrm{e}^{-\rho A_r}}\end{aligned} \tag{3}$$

在评估过程中，也有一些度量方法设定假名更换频率，计算匿名集合的平均大小，但其假设条件及计算过程复杂，目前较少文献采用。

4.2 基于熵的关联性度量

文献[18]提出了观察 mix-zone 出口事件的方法用式(4)来度量位置隐私，式中，q_{sj} 表示车辆由口 s 进入 mix-zone 口 j 离开的条件概率，$f_{sj}(t)$表示车辆在时间 t 内由 s 到 j 穿越 mix-zone 的概率，p_{jt} 表示车辆在时间 t 内由入口 s 进入、出口 j 离开 mix-zone 的概率。同一时刻车辆对不同出口的概率与均匀分布的吻合度，表明了隐私保护水平的高低。

$$p_{jt}=q_{sj}f_{sj}(t) \tag{4}$$

文献[27]假设 mix-zone 内有 N 辆车，类似均匀分布。车辆在时间 t 内由入口 s 进入、出口 j 离开 mix-zone 记为事件 l，与事件 l 相关联的位置隐私是该事件概率 p_{jt} 的熵，由式(5)表示。这个熵值依赖于 2 个因素：mix-zone 内的车辆数 N 和事件 l 的概率分布与均匀分布的相似程度，并且随着这 2 个因素的增大而增大。事件概率 p_{jt} 遵循式(4)，其中，q_{sj} 和 $f_{sj}(t)$的概率分布依赖于攻击模型。

$$H(l)=-\sum_{s=1}^{N}p_{jt}\mathrm{lb}(p_{jt}) \tag{5}$$

将式(5)中 mix-zone 内的车辆数目 N 广义表示成匿名集合中车辆的数目$|S_A|$，用式(6)[42]来表示这个熵值。其中，P_i 表示车辆 i 被选择跟踪的概率，并且 $\sum_{i=1}^{|S_A|}P_i=1$。如果 $H(p)=0$，则表示被跟踪的车辆不属于任何的匿名集合，该车辆容易被追踪。$H(p)$值越大，则表明车辆的位置隐私保护水平越高。式(6)中熵值的高低从数量的角度表明了隐私保护水平的高低。

$$H(p)=-\sum_{i=1}^{|S_A|}P_i\mathrm{lb}P_i \tag{6}$$

4.3 基于分布概率的数学理论分析

基于匿名分析，采用统计学方法，理论推导某区域的匿名程度。某个时间段内车辆匿名集合的大小表明了隐私程度，集合越大，隐私保护程度越高。文献[20,21]假设在时间段 T_s 内，车辆到达某个 small social spot 是一个泊松分布，车辆到达的时间间隔满足期望值为 1/λ的指数分布，在交通灯(small social spot)处的分析模型如式(7)~式(9)。P_r 表示在时间段 T_s 内到达路口的车辆随机分布 X 的概率；E 表示车辆分布 X 的数目；S_{anony}(匿名集合大小)等于 S_a(路口的停车数)。

$$P_r\left[X=x\,|\,T_s=t\right]=\frac{(\lambda t)^x}{x!}\mathrm{e}^{-\lambda t} \tag{7}$$

$$\mathrm{E}\left[X\,|\,T_s=t\right]=\sum_{x=1}^{\infty}xP_r[X=x\,|\,T_s=t]=\lambda t \tag{8}$$

$$S_{anony}=S_a=\mathrm{E}[X\,|\,T_s=t]=\lambda t \tag{9}$$

匿名集合分析是基于假设所有的车辆都会在 social spot 处更换假名，显然，匿名集合越大，匿名保护水平就越高。

4.4 隐私保护顽健性的形式化证明

形式化证明首先需要定义网络模型，然后利用协议分析工具(例如 ProVerif)或者推理证明来判断隐私实现程度。建立模型之后，通常需要分析隐私成立的条件并且进行形式化描述。文献[28]建立了 mix-zone 模型，并且在该模型下提出了隐私的形式化定义。Mix-zone 模型如图 4 所示，由 5 个位置构成：$entry_L$、$entry_R$、proximity、$exit_L$ 和 $exit_R$。以单个 mix-zone 内的 2 辆车 V_1、V_2 为例，V_1、V_2 分别

表 2　　主要隐私保护水平的度量方法比较

主要度量方法	方法特点	达到隐私的判断条件	使用频度	主要性能目标
匿名集合[10,20,29]	同时更换匿名的集合	匿名集合的大小不小于 1，越大则匿名程度越高	高	匿名
事件熵[18,22,27]	利用贝叶斯决策	判断某车辆出口事件的概率越大，被跟踪的概率越大	中	不可跟踪
匿名集合熵[25,31,42]	考虑集合分布状况	匿名分布熵值越高，位置匿名所达到的水平越高	高	匿名
数学理论分析[20,21]	理论推导	理论分析出的匿名集越大，匿名程度越高	低	匿名
形式化分析[28]	协议分析与证明	验证形式化定义的隐私要求，判断满足情况	低	不可跟踪

由 $entry_L$ 和 $entry_R$ 进入穿过 mix-zone，那可能存在 2 种情况：V_1 由 $exit_L$ 出，V_2 由 $exit_R$ 出；V_1 由 $exit_R$ 出，V_2 由 $exit_L$ 出。如果攻击者无法区分这 2 种情况，即式(10)成立，那么隐私性就得到了保证。针对理想模型与以 CMIX 协议[27]为基础的 CMIX 模型，若形式化分析的结果满足式(10)中的等价关系，则在模型中的情境下实现了隐私要求。

$$C[V_1(entry_L, exit_L) | V_2(entry_R, exit_R)] \cdot C[V_1(entry_L, exit_R) | V_2(entry_R, exit_L)] \quad (10)$$

式(10)中的 $V(entry,exit)$表示车辆从 entry 运动到 exit 的过程。这个等价式表示图 4 中的 2 辆车由不同的出口离开 mix-zone 时，在攻击者看来是无异的、等价的。

对隐私保护水平的度量方法总结如表 2 所示。

5　结束语

目前，车辆自组网已成为无线通信服务市场一个重要领域，基于位置服务作为车辆网络的特色支撑技术，隐私保护是其不可回避的关键问题。目前，国内已经开展了对泛在网络隐私保护技术的研究[43]，但是关于车辆网络位置服务方面，主要是提高如下载速度等服务质量[44]方面，尚未涉及隐私保护技术及其评估方法。为推进此方面的研究，本文介绍了车载自组网位置服务的基本内容；分析了主要的隐私保护技术；比较了常用的隐私度量方法。总的来说，车载网内的位置隐私已受到广泛的关注，研究逐步活跃，但尚有不少问题仍有争议，概括起来，如下几个方面的问题还需要进一步细致而深入的研究。

首先，现有的 VANET 的位置隐私保护过程大多建立在比较理想化或局限的车载环境中，如假设车流量达到一定量，场景仅限在城市交叉口、交通灯下等。虽然理想环境规范了模型的建立及简化了问题的处理，但需要进一步将实际中车辆高速移动、道路场景多样(如高速公路、车辆稀少处)、网络拓扑变化快等车载网络的特点深入考虑。

其次，假名方法使用很广泛，研究主要集中在管理、更新地点及更新策略上，而某个假名的寿命，或是说假名更新的频率对隐私的影响之间的关联度，缺乏深入的研究。而且，对失效假名的撤消与回收利用问题，在车辆自组网规模越来越大，是不可避免需要深入研究的内容。

最后，建立一个车辆自组网中位置隐私保护水平评估的通用标准，使隐私需求、隐私保护方法、系统隐私保护水平等都有一个相对统一的规范，规范的建立将是车辆自组网隐私研究的新方向。

参考文献：

[1] MOKBEL M F. Privacy in location-based services: start-of-the-art and research directions[A]. Proceedings of 8th International Conference on Mobile Data Management (MDM'07)[C]. Mannheim, Germany, 2007. 228.

[2] GEDIK B, LIN L. Protecting location privacy with personalized *k*-anonymity: architecture and algorithms[J]. IEEE Transactions on Mobile Computing, 2008, 7(1):1-18.

[3] LIU L. From data privacy to location privacy: models and algorithms[A]. Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB'07)[C]. Vienna, Austria, 2007. 1429-1430.

[4] TOOR Y, MUHLETHALER P, LAOUITI A. Vehicle ad hoc networks: applications and related technical issues[J]. IEEE Communication Surveys and Tutorials, 2008, 10(3):74-88.

[5] ZHU H J, LU R X, SHEN X M, *et al*. Security in service-oriented vehicular networks[J]. IEEE Wireless Communication, 2009, 16(4): 16-22.

[6] PAPADIMITRATOS P, BUTTYAN L, HOLCZER T, *et al*. Secure vehicular communications: design and architecture[J]. IEEE Communications Magazine, 2008, 46(11):100-109.

[7] CAPKUN S, HUBAUX J P, JAKOBSSON M. Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks[R]. EPEFL-IC Technical Report, 2004.

[8] RAYA M, HUBAUX J P. The security of vehicular ad hoc networks[A]. Proceedings of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)[C]. NY, USA, 2005. 11-21.

[9] HOH B, GRUTESER M, HUI X, *et al*. Preserving privacy in GPS traces via uncertainty-aware path cloaking[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07)[C]. 2007. 161-171.

[10] WASEF A, SHEN X M. REP: Location privacy for VANET using random encryption periods[J]. ACM Mobile Networks and Applications (MONET), 2010, 15(1): 172-185.

[11] BERESFORD A R, STAJANO F. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46-55.

[12] CHAUM D L. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2):84-90.

[13] BERESFORD A R, STAJANO F. Mix-zone: user privacy in location-aware services[A]. Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications[C]. Florida, US, 2004. 127-131.

[14] GRUTESER M, GRUNWALD D. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis[J]. Mobile Networks and Applications, 2005, 10(3):315-325.

[15] HUANG L P, YAMANE H, MATSUURA K, *et al*. Towards modeling wireless location privacy[A]. PETS[C]. 2006. 59-77.

[16] FREUDIGER J, SHOKRI R, HUBAUX J P. On the optimal placement of mix zones[A]. PETS[C]. 2009. 216-234.

[17] AIJAZ A, BOCHOW B, DOTZER F, *et al*. Attacks on inter vehicle communication systems-an analysis[A]. Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT 2006)[C]. Hamburg, Germany, 2006. 1-11.

[18] BUTTYAN L, HOLCZER T, VAJDA I. On the effectiveness of changing pseudonyms to provide location privacy in VANET[A]. Proceedings of ESAS'07[C]. 2007. 129-141.

[19] SCHEUER F, POSSE K, FEDERRATH H. Preventing profile generation in vehicular networks[A]. Proceedings of the 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communication[C]. Washington, DC, USA, 2008. 520-525.

[20] LU R X, LIN X D, LUAN T H, *et al*. Anonymity analysis on social spot based pseudonym changing for location privacy in VANET[A]. IEEE ICC'11[C]. Kyoto, Japan, 2011. 1-5.

[21] LU R X, LIN X D, LUAN T H, *et al*. Pseudonym changing at social spots: an effective strategy for location privacy in VANET[J]. IEEE Transaction on Vehicular Technology, 2012, 61(1):86-96.

[22] BUTTYAN L, HOLCZER T, WEIMERSKIRCH A, *et al*. Slow: a practical pseudonym changing scheme for location privacy in VANETs[A]. IEEE Vehicular Networking Conference (VNC)[C]. Tokyo, Japan, 2009. 1-8.

[23] HUANG L P, MATSUURA K, YAMANE H, *et al*. Enhancing wireless location privacy using silent period[A]. ECNC[C]. 2005. 1187- 1192.

[24] LI M Y, SAMPIGETHAYA K, HUANG L P, *et al*. Swing & swap: user-centric approaches towards maximizing location privacy[A]. Proceedings of the 5th ACM Workshop on Privacy in Electronic Society[C]. New York, USA, 2006. 19-28.

[25] SAMPIGETHAYA K, LI M Y, HUANG L P, *et al*. Amoeba: robust location privacy scheme for VANET[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8): 1569-1589.

[26] FREUDIGER J, MANSHAEI M H, HUBAUX J P, *et al*. On non-cooperative location privacy: a game-theoretic analysis[A]. CCS'09[C]. NY, USA, 2009.324-337.

[27] FREUDIGER J, RAYA M, FLEGYHZI M, *et al*. Mix-zone for location privacy in vehicular networks[A]. Proc of ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07)[C]. Vancouver, Canada, 2007.

[28] DAHL M, DELAUNE S, STEEL G. Formal analysis of privacy for vehicular mix-zones[A]. Proceedings of the 15th European Symposium on Research in Computer Security[C]. 2010. 55-70.

[29] SAMPIGETHAYA K, HUANG L P, LI M Y, *et al*. CARAVAN: providing location privacy for VANET[A]. ESCAR[C]. 2005.

[30] SCHEUER F, FUCHS K P, FEDERRATH H. A safety-preserving mix zone for VANET[A]. Trust, Privacy and Security in Digital Business[C]. Berlin Heidelberg, 2011. 37-48.

[31] SUN Y P, SU X Y, ZHAO B K, *et al*. Mix-zones deployment for location privacy preservation in vehicle communications[A]. IEEE 10th International Conference on Compute and Information Technology (CIT 2010)[C]. Bradford, England, 2010. 2825-2830.

[32] CHAUM D, HEYST E V. Group signatures[A]. Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques[C]. Berlin, Heidelberg, 1991. 257-265.

[33] BONEH D, BOYEN X, SHACHAM H. Short group signatures[A]. CRYPTO 2004[C]. Berlin, Heidelberg, 2004. 227-242.

[34] NAKANISHI T, FUNABIKI N. Verifier-local revocation group signature schemes with backward unlinkability from billing maps[A]. ASIACRYPT 2005[C]. Chennai, India, 2005. 533-548.

[35] ZHANG J L, MA L ZH, SU W L, *et al*. Privacy-preserving authentication based on short group signature in vehicular networks[A]. ISDPE 2007[C]. Chengdu, China, 2007. 138-142.

[36] LU R X, LIN X D, LIANG X H, *et al*. A dynamic privacy-preserving

key management scheme for location based services in VANET[J]. IEEE Transactions on Intelligent Transportation Systems, 2011, 13(1):127-139.

[37] LIN X D, SUN X T, HO P H, *et al*. GSIS: a secure and privacy-preserving protocol for vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442-3456.

[38] LU R X, LIN X D, ZHU H J, *et al*. ECPP: efficient condition privacy preservation protocol for secure vehicular communications[A]. IEEE INFOCOM 2008[C]. Phoenix, AZ, 2008. 1229-1237.

[39] LU R X, LIN X D, SHEN X M. Spring: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks[A]. INFOCOM 2010[C]. California, USA, 2010. 1-9.

[40] SCHECHTER S, PARNELL T, HARTEMINK A. Anonymous authentication of membership in dynamic groups[A]. Proceedings of the Third International Conference on Financial Data Security and Digital Commerce[C]. 1999. 184-195.

[41] CHAURASIA B K, VERMA S. Conditional privacy through ring signature in vehicular ad-hoc networks[A]. Transactions on Computational Science[C]. Berlin, Heidelberg, 2011. 147-156.

[42] WEI Y C, CHEN Y M, SHAN H L. RSSI-based user centric anonymization for location privacy in vehicular networks[J]. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, 42(2): 39-51.

[43] 李大伟, 杨庚, 苏弘逸等. 基于身份的泛在通信隐私保护方案[J], 通信学报, 2011,32(9):44-50.
LI D W, YANG G, SU H Y, *et al*. Identity based privacy preservation scheme for ubiquitous computing[J]. Journal on Communications, 2011, 32(9):44-50.

[44] 刘建航, 孙江明, 毕经平等. 基于动态时槽的车联网协助下载方法研究[J]. 计算机学报, 2011, 34(8):1378-1386.
LIU J H, SUN J M, BI J P, *et al*. VANET cooperative downloading approach study based on dynamic slot[J]. Chinese Journal of Computers, 2011, 34(8):1378-1386.

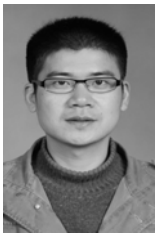
作者简介：

张建明（1964-），男，江苏镇江人，江苏大学教授，主要研究方向为物联网与安全协议。

赵玉娟（1984-），女，江苏南通人，江苏大学硕士生，主要研究方向为无线传感器网络安全。

江浩斌（1969-），男，江苏启东人，江苏大学教授、博士生导师，主要研究方向为道路物流车辆运行组织与监控技术。

贾雪丹（1988-），女，山东德州人，江苏大学硕士生，主要研究方向为车载网络安全与隐私保护。



王良民（1977-），男，安徽潜山人，江苏大学副教授、硕士生导师，主要研究方向为物联网安全与隐私保护技术。