计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190314
56(10): 2277-2286, 2019

一种安全高效的无人驾驶车辆地图更新方案

赖成喆 张 敏 郑 东
(西安邮电大学无线网络安全技术国家工程实验室 西安 710121)
(lcz_xupt@163.com)

A Secure and Efficient Map Update Scheme for Autonomous Vehicles

Lai Chengzhe, Zhang Min, and Zheng Dong
(*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121)

Abstract Real-time map plays an important role in autonomous vehicles (AVs) navigation. Compared with the existing map updating methods, the real-time map updating method is based on crowdsensing has lower cost and higher accuracy. However, in the process of map updating, this method increases the risk of data and user identity leakage. How to ensure the confidentiality of uploaded data and the anonymity of users is a challenge in real-time map updating. This paper proposes a secure and efficient map update scheme for AVs (SEMU). In the SEMU, vehicle users can sign the sensing data and store the encrypted data in the vehicular fog node by using signcryption and proxy re-encryption technology. When the map company wants to access the data, the vehicular fog node sends the encrypted data to the server, and the server re-encrypts the data to the map company. At the same time, server cannot obtain any explicit information about the data. In addition, the aggregate signature technology is applied to reduce the computational overhead. Through the credit management of vehicle users, the reliability of data can be improved. Finally, security analysis shows that the scheme achieves data confidentiality, integrity, reliability, authentication and non-repudiation, and guarantees the anonymity and traceability of users. The simulation results illustrate that the proposed SEMU has the incentive, and it is efficient in terms of computational overhead.

Key words proxy re-encryption; vehicle map update; aggregate signature; signcryption; autonomous vehicles (AVs); secure and efficient map update scheme for AVs (SEMU)

摘 要 实时地图在无人驾驶车辆导航中发挥着至关重要的作用.和现有的地图更新方法相比,基于群智感知的实时地图更新方法成本更低且准确性更高.然而,此方法在地图更新过程中,会增加数据及用户身份泄露的风险.如何保证上传数据的机密性和用户的匿名性是实时地图更新中的一个挑战.提出了一种安全高效的无人驾驶车辆地图更新方案(secure and efficient map update scheme for AVs, SEMU).在SEMU方案中,利用签密和代理重加密技术,车辆用户对感知数据进行签密,将加密的数据存储在车辆雾节点中,当地图公司希望访问数据时,雾节点将加密的数据发送给云服务平台,云服务平

收稿日期:2019-05-30;**修回日期**:2019-08-01
基金项目:国家自然科学基金项目(61872293);陕西省创新人才推进计划项目(2017KJXX-47);西安邮电大学研究生创新基金项目(CXJJLA2018004)
This work was supported by the National Natural Science Foundation of China (61872293), the Innovation Ability Support Program in Shaanxi Province of China (2017KJXX-47), and the Graduate Innovation Fund of Xi'an University of Posts & Telecommunications (CXJJLA2018004).
通信作者:张敏(bk187151@163.com)

台重新加密数据发送给地图公司,同时,云服务平台无法获得任何有关数据的明文信息.利用聚合签名技术,降低了计算开销.通过对车辆用户的信誉管理,提高了数据的可靠性.最后,安全性分析表明该方案实现了数据的机密性、完整性、可靠性、身份可验证性和不可否认性,保证了用户的匿名性和可追踪性.仿真验证了方案的激励性,并从计算开销方面证明了它的有效性.

关键词 代理重加密;车辆地图更新;聚合签名;签密;无人驾驶车辆;安全高效的无人驾驶车辆地图更新方案

中图法分类号 TP309

近年来,人工智能技术的迅速发展,使得传统汽车行业与信息技术相结合,促进了无人驾驶领域的进一步发展.无人驾驶车辆可以通过大幅减少撞车事故来缓解交通拥堵[1],从根本上缓解交通压力[2],也可使老年人[3]和残障人士[4]的出行更加便利.然而,无人驾驶车辆必须从车辆地图上访问大量数据,以便为安全和效率做出实时控制决策[5],这使得车辆地图成为无人驾驶发展的关键.

地图对无人驾驶车辆的定位、导航与控制以及数据的实时更新都起着至关重要的作用,为无人驾驶车辆提供了更加可靠的感知能力.目前,基于卫星图像的数字地图得到了广泛的应用,但是,它们不能准确地反映最新的地图数据.为了准确有效地反映地图的最新动态,近年来提出了许多方案[6-8],其中基于群智感知的地图更新方法最引人关注[9-10].在这些方案中,志愿者愿意将他们的GPS数据贡献给地图服务器,但是同时也增加了用户隐私泄露的风险.由于数据安全问题以及用户担心隐私被泄露[11],使得车辆地图更新的发展受到了严重影响.当用户通过网络进行数据交互时,数据的所有者不再对数据具有控制权,而是托管到了云端进行进一步的运算及处理,所以如何保障托管数据的完整性和机密性便成了云端所面临的全新挑战.云服务平台流通的数据量与日俱增,其中包含了大量的敏感数据和隐私信息,这使得车辆用户的隐私问题尤为凸显.

针对以上问题,本文将代理重加密和签密的思想引入到车辆地图的更新中,提出了一种安全高效的无人驾驶车辆地图更新方案(secure and efficient map update scheme for AVs, SEMU),它实现了数据的机密性、完整性、可靠性、身份可验证性和不可否认性.由于存在隐私被泄露的风险,用户经常不愿意上传数据.所以本文通过为用户生成伪名,实现了用户的匿名性和有条件的隐私.具体来说,本文的主要贡献有3个方面:

1) 提出一种安全高效的无人驾驶车辆地图更新方案,实现了数据的机密性、完整性、身份可验证性和不可否认性,保证了用户的匿名性和可追踪性;

2) 通过对用户信誉值的管理,提高了数据可靠性,利用聚合签名技术,降低了计算开销;

3) 通过仿真,验证了方案的激励性,并从计算开销方面证明了它的有效性.

1 相关工作

在群智感知网络中进行数据共享时,数据所有者需要先将数据进行加密,云服务平台再对云端密文进行解密,最后将解密后的数据重新加密分享给数据使用者,然而这个方法使得用户数据极易遭到泄露且计算效率低.因此必须设计合理的隐私保护机制来保证数据安全的同时也能够保护用户的隐私.

为了实现加密数据的高效分享,Blaze等人[12]在1998年的欧密会上首次提出了代理重加密(proxy re-encryption, PRE)的概念.在代理重加密系统中,一个拥有重加密密钥的半可信代理,能够将通过数据提供者的公钥加密得到的密文,转换为被数据使用者的公钥加密的密文,在此过程中代理不知道有关数据的任何明文信息.此外,这2个不同的密文所对应的明文是一致的.因此,代理重加密技术是实现数据高效共享的一种有效途径,并引起了学术界的普遍关注,相继出现了很多代理重加密方案.

2007年Green和Ateniese[13]将该概念扩展到基于身份的密码系统,将基于身份的密码体制(identity-based cryptosystem, IBC)和PRE结合起来,首次提出基于身份的代理重加密(identity-based proxy re-encryption, IBPRE)的概念.Kirtane和Rangan[14]使用Malone-Lee和Mao[15]的方案,构造了一个具有代理重加密功能的签名方案.代理可以在不使用数据所有者私钥的情况下,将数据所有者

已签名的密文重新加密为数据使用者的另一个密文.之后在文献[16-18]中提出了3种具有代理重加密功能的基于身份的签密(identity-based signcryption, IBSC)方案.然而,CAR方案[16]和WC方案[17]对适应性选择密文攻击都不安全,而文献[19]中的方案对适应性选择密文攻击是安全的.因此,构建一个具有代理重加密功能的且安全高效的IBSC方案显得尤为重要.

云存储[20]中的数据访问控制方案还可以通过使用预加密和基于属性的加密方案(attribute-based encryption, ABE)来设计.Li等人[21]提出一种针对云服务存储的灵活的ABE机制.文献[22]进一步阐述了密文策略属性基加密方案(ciphertext-policy attribute-based encryption, CP-ABE)在云计算环境中的应用策略.但是CP-ABE机制中针对数据授权的变更问题,仍需要用户对数据进行重复加密.

PRE技术在一定程度上满足了云端数据[23]的机密性和完整性的安全管理需求.然而,云计算中的数据存储还需要满足身份可验证性、可靠性和不可否认性.

2 准备工作

2.1 双线性映射

设q是一大素数,G_1和G_2是2个阶为q的群,其上的运算分别为加法和乘法.G_1和G_2的双线性映射$\hat{e}:G_1\times G_1\to G_2$,满足3个性质:

1) 双线性

如果对任意$P,Q\in G_1$和$a,b\in Z$,有:

$$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab},$$

那么就称该映射为双线性映射.

2) 非退化性

映射不把$G_1\times G_1$中的所有元素对(即序偶)映射到G_2中的单位元,由于G_1,G_2都是阶为素数的群,这意味着:如果P是G_1的生成元,那么$\hat{e}(P,P)$就是G_2的生成元.

3) 可计算性

对任意的$P,Q\in G_1$,存在一个有效算法计算$\hat{e}(P,Q)$.

2.2 困难问题

离散对数问题:G_1为一个阶为素数q的循环群,P为其生成元,对于$b\in G_1^*$,找到整数a,使得$b=aP$是困难的.

计算性Diffie-Hellman(CDH)问题:G_1为一个阶为素数q的循环群,P为其生成元,已知(aP,bP),计算abP是困难的.

2.3 IBSC方案概述

IBSC方案的工作原理[19]如图1所示:

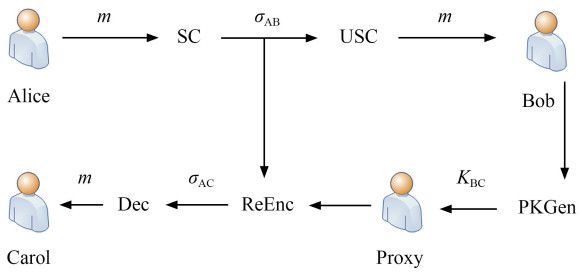

Fig. 1 Working principles of IBSC scheme

图1 IBSC方案工作原理[19]

1) 签密(signcryption, SC).数据所有者Alice为发起方,Alice将明文m通过自己的私钥S_{ID_A}和Bob的身份ID_B进行签密,生成一级密文σ_{AB}.

2) 解签密(unsigncryption, USC).将Alice的身份ID_A和一级密文σ_{AB}作为输入,Bob可以通过自己的私钥S_{ID_B}得到明文m.

3) 代理密钥生成(proxy key generation, PKGen).Bob通过自己的私钥S_{ID_B}和Carol的身份ID_C,生成代理密钥K_{BC}.

4) 重加密(re-encryption, ReEnc).代理中心将Proxy一级密文σ_{AB}和代理密钥K_{BC}作为输入可生成二级密文σ_{AC}.

5) 解密(decryption, Dec).Carol可以通过自己的私钥S_{ID_C}及Alice和Bob的身份ID_A,ID_B解密得到明文m.

3 群智模型

群智感知[24-25]的系统结构[24]如图2所示,该系统结构包括3部分:任务参与者(数据提供者)、数据使用者和服务器平台.服务器平台接受来自数据使用者的服务请求,将感知任务分配给任务参与者,处理收集到的感知数据,并进行其他的管理功能.任务参与者接收到任务后,进行所需数据的感知,然后将数据报告返回给服务器平台,服务器平台将数据处理后发送给数据使用者.通过整个流程实现了数据感知、数据收集以及信息服务提供等功能.群智感知是一种移动的、分布式的、自主的、基层的服务模式.

群智感知可以从各地收集海量多维异构数据,解决各种大规模地数据需求问题,提供高质量且可

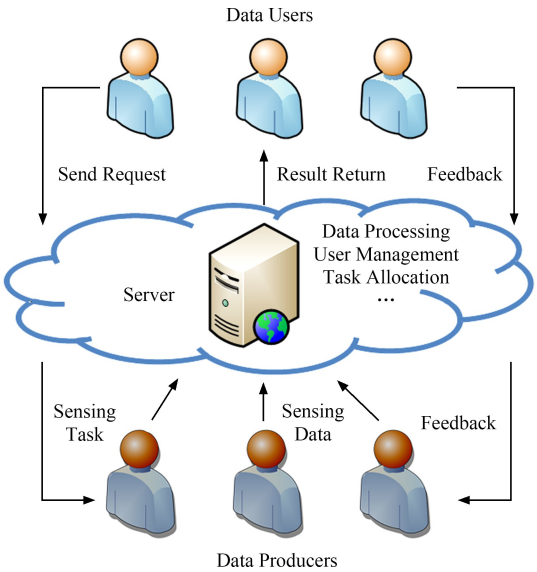

Fig. 2 Architecture of a crowd sensing system

图 2 群智感知系统结构[24]

靠的数据服务.但是,随着群智感知的发展,新的问题和挑战也逐渐显现出来.其中,数据安全和用户隐私安全问题尤为突出.在群智感知中,用户提交的数据可能会包含用户的敏感信息,只有降低隐私泄露[26]的风险才可以激励用户积极地参与感知任务.数据安全是指在数据传送的过程中保证数据的保密性、完整性、可靠性、身份可验证性和不可否认性.

4 本文方案

4.1 系统模型

在本文安全高效的无人驾驶车辆地图更新方案SEMU中,地图公司将感知任务外包给云服务平台,并奖励为感知任务做出贡献的车辆用户.云服务平台将任务释放给位于感测区域的车辆雾节点.根据任务,车辆雾节点找到正确的感知报告,如果有所需数据,则将其返回到云服务平台;反之车辆雾节点则会继续广播此任务.愿意参与的车辆用户将加密数据和同意自己数据的 n 个其他车辆用户的聚合签名发送给车辆雾节点,车辆雾节点对此聚合签名进行批量验证.验证通过后,将加密数据发送给云服务平台.利用代理中心生成的代理密钥,云服务平台对加密数据进行代理重加密[19],然后将重加密后的数据发送给地图公司.最后,地图公司解密得到数据内容,并对提交有价值数据的车辆用户分配奖励.图3描述了本文提出的方案的系统模型,它主要由7部分组成:

1) 地图公司(map company, MC).地图公司需要完成大量的数据收集任务来更新地图,但他们没有足够的能力独自完成任务.因此,地图公司向云服务平台发放任务,之后再通过云服务平台获取感知

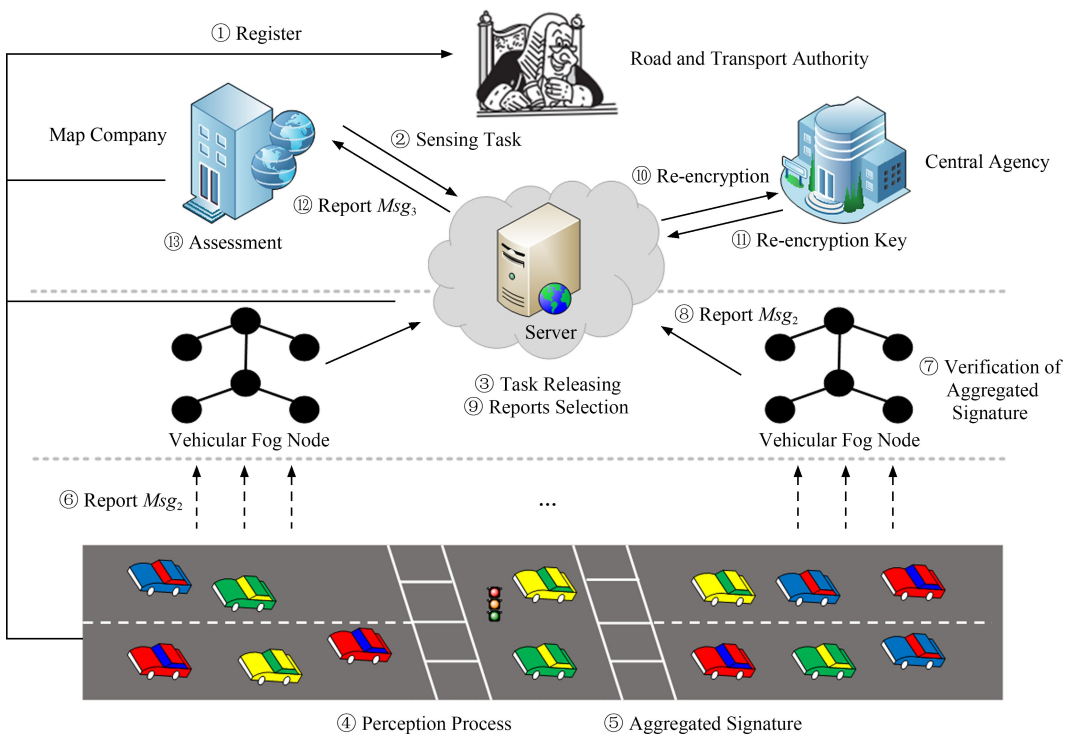

Fig. 3 The system model—SEMU

图 3 SEMU 系统模型

数据并进行解密,最终得到感知数据并对完成任务的车辆给予奖励.

2) 车辆(vehicular user, V_i).现在的车辆设备部署了丰富的计算、通信和存储资源且有很强的移动性.车辆确保他们的设备有足够的能力支持正常功能.他们参与任务进行收集数据,并对其进行签密等处理,最终通过云服务平台进行数据共享以获得信誉值或报酬.

3) 云服务平台(server).他们有足够的存储和计算资源来提供众包服务.云服务平台接收来自地图公司的任务,并将任务发放给位于感测区域的车辆雾节点.收集到雾节点的报告后,根据车辆的信誉值选择报告,为地图公司生成结果.

4) 车辆雾节点(vehicular fog node, VFN).批量验证车辆发送来的聚合签名.根据云服务平台发放的任务,雾节点找到正确的感知报告,如果有所需的数据,则将其发放给云服务平台.

5) 代理中心(central agency, CA).代理中心为云服务平台生成所需的代理密钥,监视所有用户之间的交互,并更新他们的信誉值,然后将用户的信誉广播给每个参与者.此外,代理中心还检查感知数据是否被地图公司成功接受.

6) 道路交通管理局(road and transport authority, RTA).车辆需到 RTA 处登记注册.为保护车辆的隐私,RTA 为每个车辆用户生成对应的伪身份.当要追查违规的车辆时,RTA 可出示或曝光车辆的真实身份.

7) 密钥生成中心(private key generator, PKG).为每个车辆用户生成对应的私钥.

4.2 方案描述

1) 系统建立

密钥生成中心(PKG)选择一安全参数 k,加法循环群 G_1 和乘法循环群 G_2 的阶为素数 $q>2^k$,这 2 个循环群满足的双线性映射为 $\hat{e}:G_1\times G_1\rightarrow G_2$,群 G_1 的生成元是 P;其次,PKG 随机选择主密钥 $s\in Z_q^*$,计算 $P_{\text{pub}}=sP$.然后选择安全的 Hash 函数 $H_1,H_3,H_4:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\rightarrow Z_p^*$.最后,PKG 公开系统的参数列表$(G_1,G_2,\hat{e},P,P_{\text{pub}},H_1,H_2,H_3,H_4)$.

2) 车辆注册

车辆需到道路交通管理局(RTA)处登记.为保护用户的隐私,对身份为 ID_i 的用户,RTA 为其生成伪身份 Q_{ID_i},RTA 选择 $H_1:\{0,1\}^*\rightarrow G_1$,计算 $ID_i'=H_1(ID_i)$,$Q_{ID_i}=H_1(ID_i')$.当要追查违规车辆时,RTA 可出示或曝光用户的真实身份.

3) 密钥生成

车辆发送 Q_{ID} 给 PKG,PKG 计算用户私钥 $S_{ID}=sQ_{ID}$.

4) 任务发放

地图公司将任务 $task_i=\{j,Q_{ID_C},type,area,cr\}$外包给云服务平台,其中包括任务编号 j、公司的伪名 Q_{ID_C}、数据类型要求 $type$、任务的大致区域 $area$ 和此次任务对车辆用户要求的信誉阈值 cr.地图公司通过支付报酬,去奖励来自某一车辆的报告.云服务平台收到后根据任务要求的区域将任务分别分发给车辆雾节点.根据任务,雾节点找到正确的感知报告,如果有所需的数据,则将其返回到云服务平台,反之雾节点继续广播此任务.

5) 数据收集

为了提高数据的可靠性,愿意参与感知任务且满足任务信誉值要求的车辆 V_A 邀请数据路况周围的一组车辆$(V_1,V_2,\cdots,V_n)$(通过信誉阈值来规定 n 值,详见 4.2 节)同意其带有相应签名的感知数据 m.$V_1,V_2,\cdots,V_n$ 先验证车辆 V_A 的签名是否有效,验证通过后,若不同意 m,可及时举报车辆 V_A.RTA 经过调查,确认车辆 V_A 违规,CA 将增加举报用户的信誉值,减少车辆 V_A 以及同意数据 m 的车辆用户的信誉值.若车辆多次违规,RTA 将撤销其身份;反之,若同意 m,$V_1,V_2,\cdots,V_n$ 则对此数据 m 签名.车辆 V_A 验证每个车辆的签名,对于验证通过的车辆,车辆 V_A 支付报酬作为对其的奖励.最后,车辆 V_A 将 n 个签名进行聚合[27],并发送给车辆雾节点.具体过程如下:

① 签名.ID_i' 随机选取 $r\in Z_p^*$,计算:

$$X=rQ_{ID_A},$$

$$h=H_2(X,m),$$

$$Z_A=(r+h)S_{ID_A},$$

得到签名(Z_A,P).

② 验证签名.车辆 V_A 向数据路况周围的一组车辆$(V_1,V_2,\cdots,V_n)$广播报告 $Msg_1=\{m\parallel(Z_A,P)\}$,同意数据 m 的车辆用户通过 $\hat{e}(Z_A,P)=\hat{e}(X+hQ_{ID_A},P_{\text{pub}})$验证车辆 V_A 的签名(Z_A,P),如果成立,其他车辆用户对数据 m 进行签名.

③ 聚合签名.车辆 V_A 将 n 个车辆用户的签名进行聚合,首先车辆 V_A 对每个车辆的签名(Z_i,P) $(1\leqslant i\leqslant n)$进行验证,验证通过后则生成聚合签名

$\left(\sum_{i=1}^{n} Z_i, P\right)$.一旦验证算法失败或某个车辆违规时,用户即可把违规车辆的伪身份递交给 RTA,RTA 可出示或曝光车辆用户的真实身份.

④ 签密算法.车辆 V_A 计算:

$$w=\hat{e}(r S_{ID_A}, Q_{ID_B}),$$
$$y=m w,$$
$$U=H_3(X, Z_A, y, ID'_A, ID'_B),$$
$$V=r U,$$
$$\sigma_{AB}=(X, Z_A, y, V),$$

其中,Q_{ID_B}为 CA 的伪名,σ_{AB}为一级密文.车辆 V_A 将报告 $Msg_2=\{j, \sigma_{AB}, ID'_A, ID'_C, cr_A\}$以及聚合签名$\left(\sum_{i=1}^{n} Z_i, P\right)$发送给车辆雾节点.雾节点通过 $\hat{e}\left(\sum_{i=1}^{n} Z_i, P\right)=\hat{e}\left(\sum_{i=1}^{n} X+h Q_{ID_i}, P_{pub}\right)$进行批量验证,如果验证通过,雾节点将报告 Msg_2 发送给云服务平台.

6) 代理重加密

云服务平台根据车辆用户信誉值对报告进行选择,并将地图公司伪名 ID'_C 发送给代理中心 CA,使其生成重加密密钥.

① 重加密密钥生成.CA 计算:

$$W=H_4(\hat{e}(S_{ID_B}, Q_{ID_C}), ID'_B, ID'_C),$$
$$K_{BC}=W-S_{ID_B}.$$

云服务平台通过重加密密钥 K_{BC} 对一级密文 σ_{AB}进行重加密,生成地图公司可以解密的二级密文 σ_{AC}.

② 重加密.云服务平台计算:

$$U=H_3(X, Z_A, y, ID'_A, ID'_B).$$

验证 $\hat{e}(V, Q_{ID_A})=\hat{e}(U, X)$,如果验证通过,计算:

$$y'=y\hat{e}(X, K_{BC}),$$
$$\sigma_{AC}=(X, Z_A, y'),$$

其中,云服务平台通过 $\hat{e}(V, Q_{ID_A})=\hat{e}(U, X)$检验密文的有效性,平台拒绝重加密无效的密文.若验证通过,云服务平台生成二级密文 σ_{AC},并将报告 $Msg_3=\{j, \sigma_{AC}, ID'_A, ID'_B, ID'_c, cr_A, area\}$发送给地图公司.

7) 解密

地图公司计算:

$$W=H_4(\hat{e}(Q_{ID_B}, S_{ID_C}), ID'_B, ID'_C),$$
$$w'=\hat{e}(X, W),$$
$$m=y'(w')^{-1},$$
$$h=H_2(X, m).$$

最终,地图公司解密得到数据 m.通过计算 $h=H_2(X, m)$,$\hat{e}(Z_A, P)=\hat{e}(X+h Q_{ID_A}, P_{pub})$可以对数据的完整性以及数据源进行身份验证.

8) 报酬奖励

地图公司对报告进行评估,得到有价值的数据,对对应的数据提供者进行报酬奖励.

代理中心 CA 检查感知数据是否被地图公司成功接受.若接收,CA 增加并更新车辆 V_A 和帮助车辆 V_A 的 n 个其他车辆用户的信誉值,然后将用户的信誉广播给每个参与者.

5 安全性和性能分析

5.1 安全性分析

1) 正确性

① 单个签名的正确性

$$\hat{e}(Z_A, P)=\hat{e}((r+h) S_{ID_A}, P)=$$
$$\hat{e}((r+h)s Q_{ID_A}, P)=$$
$$\hat{e}((r+h) Q_{ID_A}, s P)=$$
$$\hat{e}(r Q_{ID_A}+h Q_{ID_A}, P_{pub})=$$
$$\hat{e}(X+h Q_{ID_A}, P_{pub}).$$

② 聚合签名的正确性

$$\hat{e}\left(\sum_{i=1}^{n} Z_i, P\right)=\hat{e}\left(\sum_{i=1}^{n}(r+h) S_{ID_i}, P\right)=$$
$$\hat{e}\left(\sum_{i=1}^{n}(r+h)s Q_{ID_i}, P\right)=$$
$$\hat{e}\left(\sum_{i=1}^{n}(r+h) Q_{ID_i}, s P\right)=$$
$$\hat{e}\left(\sum_{i=1}^{n} r Q_{ID_i}+h Q_{ID_i}, P_{pub}\right)=$$
$$\hat{e}\left(\sum_{i=1}^{n} X+h Q_{ID_i}, P_{pub}\right).$$

证明该方案是正确的.

2) 机密性

机密性是指除了数据拥有者及数据使用者外的其他人都不知道数据的内容.在本文中,车辆用户对感知数据进行签密,将加密的数据存储在车辆雾节点中,当地图公司希望访问数据时,雾节点将加密的数据发送给云服务平台,车辆用户委托云重新加密数据,只有经过授权的地图公司才能解密数据,云服务平台无法获得任何有关数据的明文信息.

3) 完整性

完整性是地图公司确保来自云服务平台的数据没有被篡改.地图公司利用自己的私钥解密得到数据 m,通过计算:

$$h=H_2(X,m),$$

$$\hat{e}(Z_A,P)=\hat{e}(X+h\,Q_{ID_A},P_{pub}),$$

可以对数据的完整性进行验证.

4) 身份可验证性

身份可验证性是确保只有有效的数据所有者和其他车辆用户才能参与感知任务.在本文中,通过计算 $\hat{e}(Z_A,P)=\hat{e}(X+h\,Q_{ID_A},P_{pub})$ 可对用户身份进行验证.

5) 不可否认性

不可否认性是防止数据所有者否认以前上传的数据.也就是说,如果数据所有者已将数据上载到云服务平台,则它不能否认此操作.

6) 匿名性

车辆在进行通信之前,每台车辆都会用它的真实身份 ID_i 在道路交通管理局 RTA 注册,RTA 选择 $H_1:\{0,1\}^*\rightarrow G_1$,计算车辆用户的伪身份 Q_{ID_i},除 RTA 之外不会有任何第三方知道车辆用户的真实身份.在整个通信过程中,参与的车辆以伪身份动态地加入签名过程,车辆能够在不泄露自身隐私的情况下进行匿名的信息交互,满足了匿名性要求,保护了车辆用户的身份隐私.

7) 可追踪性

RTA 可对车辆执行违规追踪.如果车辆用户在通信过程中出现发布违规信息、签名验证算法失败等情况,RTA 经过调查,确认某车辆确实存在违规行为后,可出示或曝光车辆的真实身份.RTA 利用 Hash 函数的单向性,计算车辆用户的伪身份 $ID'_i=H_1(ID_i)$,$Q_{ID_i}=H_1(ID'_i)$ 来验证车辆的真实身份.避免伪名使用的失控,并且不用储存任何伪名证书,节省了 RTA 的存储开销.

8) 数据可靠性

本文方案中只有满足地图公司信誉要求的车辆用户才可参加感知任务,同时需要车辆用户邀请数据路况周围的一组车辆用户 $(V_1,V_2,\cdots,V_n)$ 同意其带有相应签名的数据.最后,云服务平台根据用户的信誉选择合适的报告,有效地提高了数据的可靠性.

5.2 性能分析

1) 激励性

本文选择使用归一化正切函数[28]作为签名人数 n 映射到信誉阈值 cr 的函数为

$$cr=\frac{\arctan(n-\beta)+\arctan\beta}{\pi/2+\arctan\beta}.$$

有此可得:

$$n=\beta+\tan(cr(\pi/2+\arctan\beta)-\arctan\beta).$$

图 4 表示此函数的曲线.由图 4 可知,当地图公司要求的信誉阈值 $cr=0.5$ 时,信誉值高(high credit users, HCU)的用户只需收集 10 个用户的签名证明其数据可靠性即可,信誉值中等的用户(medium credit users, MCU)需要收集 15 个用户的签名,信誉值低的用户(low credit users, LCU)需要收集 20 个用户的签名.这种机制激励用户保持较高的参与度和可信度.

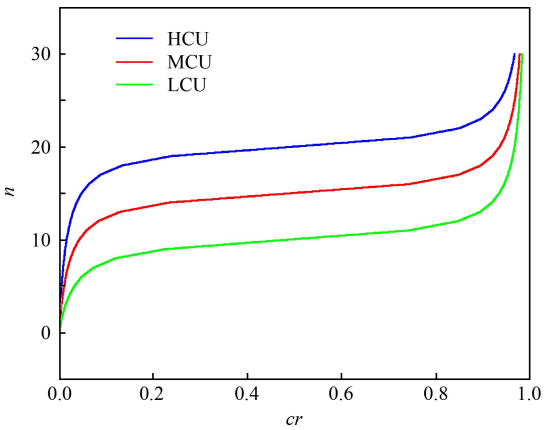

Fig. 4 Signature number calculation function curve

图 4 签名人数计算函数曲线

2) 计算效率

对于本文采用的 IBSC 方案[19]来说,计算时间和密文大小是影响计算效率的 2 个重要因素.我们将本文的 SEMU 方案的计算效率与 CAR 方案[16]和 WC 方案[17]的计算效率进行了比较.同时,本文使用的聚合签名技术也降低了计算开销.

表 1 列举了这 3 种方案的计算时间.我们用 M 表示一个标量乘运算,E 表示一个指数运算,P 表示一个双线性运算.我们选用由 8 GB 处理器内存的 Intel I5-5200 和 Windows7 组成的硬件平台,通过仿真实验结果对比了各方案的计算开销,对比结果如图 5 所示.

Table 1 Computational Time of Three Schemes

表 1 3 种方案的计算时间

Schemes	SC	PKGen	ReEnc	Dec
CAR[16]	2M+E+P	P	P	M+4P
WC[17]	2M+2P	P	P	M+5P
SEMU	4M+P	P	3P	M+4P

表 2 列举了这 3 种方案的密文大小.我们用 $|x|$ 表示 x 的位数.对于密文大小,CAR 方案和 WC 方案是相同的.一级密文和二级密文的大小都是 $2|G_1|+$

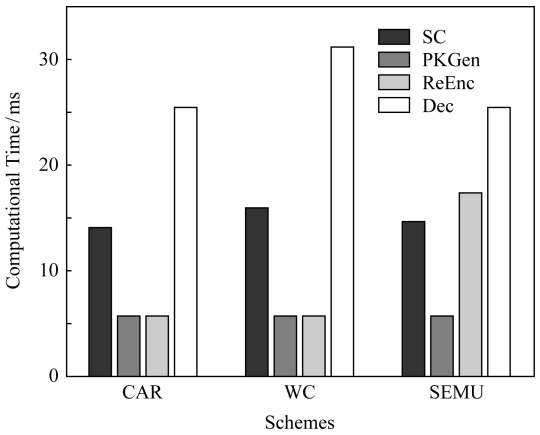

Fig. 5 Comparison of computational time of three schemes

图 5 3 种方案的计算时间比较

$|G_2|+|m|$.在我们的方案中,一级密文大小为 $3|G_1|+|G_2|$,二级密文大小为 $2|G_1|+|G_2|$.我们假设消息的大小为 $|m|=160$ b.当采用 80 b 安全级别时,$q=512$ b.所以群 G_1 中元素的大小是 1 024 b[19].通过标准压缩技术[29],群 G_1 中元素的大小可以减少到 65 B.群 G_2 中元素的大小为 1 024 b.所以,$2|G_1|+|G_2|+|m|=2\times65+128+20=278$ B,$3|G_1|+|G_2|=3\times65+128=323$ B,$2|G_1|+|G_2|=2\times65+128=258$ B.3 种方案的密文大小如图 6 所示.

Table 2 Ciphertext Size of Three Schemes

表 2 3 种方案的密文大小

Schemes	First-level Ciphertext	Second-level Ciphertext
CAR[16]	$2\|G_1\|+\|G_2\|+\|m\|$	$2\|G_1\|+\|G_2\|+\|m\|$
WC[17]	$2\|G_1\|+\|G_2\|+\|m\|$	$2\|G_1\|+\|G_2\|+\|m\|$
SEMU	$3\|G_1\|+\|G_2\|$	$2\|G_1\|+\|G_2\|$

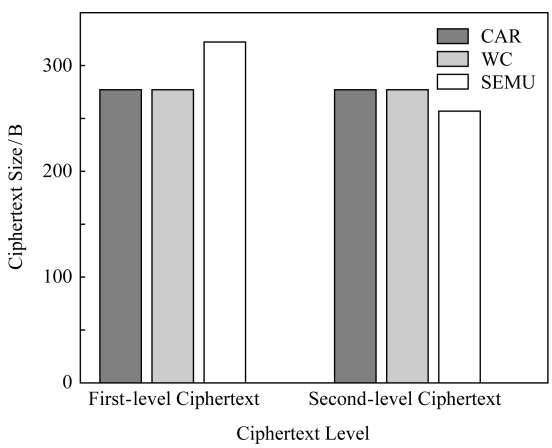

Fig. 6 Comparison of ciphertext size of three schemes

图 6 3 种方案的密文大小比较

表 3 列举了本方案单个签名验证和聚合签名验证的计算开销.聚合签名技术是将很多不同用户的签名聚合成为一个签名,只需对聚合后的签名进行验证即可判断收到签名的合法性,极大地提高了消息验证的效率.通过仿真实验结果对比了它们的计算开销,对比结果如图 7 所示.

Table 3 Computational Time of Single Verification and Aggregated Verification

表 3 单个验证和聚合验证的计算时间

Verification	Computational Time
Single Verification	nM+2nP
Aggregated Verification	nM+2P

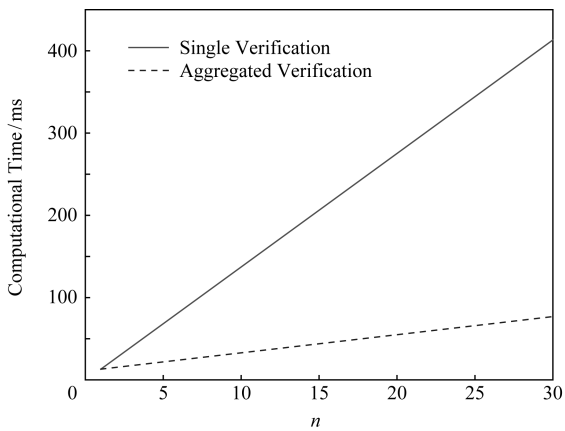

Fig. 7 Comparison of computational time between single verification and aggregated verification

图 7 单个验证和聚合验证的计算时间比较

实验分析结果表明:相对于单个签名验证,聚合签名验证具有计算开销低等优点,因此更适合于车联网等资源受限的网络环境中.

6 总 结

本文针对无人驾驶车辆地图更新中的隐私安全问题,提出了一种安全高效的无人驾驶车辆地图更新方案.本文利用签密和代理重加密技术,实现了数据的机密性、完整性、身份可验证性和不可否认性;引入信誉阈值,提高了数据的可靠性;利用聚合签名技术,降低了计算开销.为了保护用户的隐私,本文通过为用户生成伪名,实现了用户的匿名性和可追踪性.最后,通过仿真,验证了方案的激励性,并从计算开销方面证明了它的有效性.

参 考 文 献

[1] Alessandrini A, Campagna A, Delle Site P, et al. Automated vehicles and the rethinking of mobility and cities [J]. Transportation Research Procedia, 2015, 5: 145-160

[2] Bonnefon J F, Shariff A, Rahwan I. The social dilemma of autonomous vehicles [J]. Science, 2016, 352(6293): 1573-1576

[3] Yang J, Coughlin J F. In-vehicle technology for self-driving cars: Advantages and challenges for aging drivers [J]. International Journal of Automotive Technology, 2014, 15(2): 333-340

[4] Weinberger N, Winkelmann M, Müller K, et al. Public participation in the development process of a mobility assistance system for visually impaired pedestrians [J]. Societies, 2019, 9(2): 32:1-32:15

[5] Hadian M, Altuwaiyan T, Liang Xiaohui. Privacy-preserving time-sharing services for autonomous vehicles [C] //Proc of the 86th Vehicular Technology Conf (VTC-Fall). Piscataway, NJ: IEEE, 2017: 1-5

[6] Demir İ, Hughes F, Raj A, et al. Generative street addresses from satellite imagery [J]. ISPRS International Journal of Geo-Information, 2018, 7(3): 84:1-84:22

[7] Demir I, Koperski K, Lindenbaum D, et al. Deepglobe 2018: A challenge to parse the earth through satellite images [C] //Proc of 2018 IEEE/CVF Conf on Computer Vision and Pattern Recognition Workshops (CVPRW). Piscataway, NJ: IEEE, 2018: 172-17209

[8] Wang Yin, Liu Xuemei, Wei Hong, et al. Crowdatlas: Self-updating maps for cloud and personal use [C] //Proc of the 11th Annual Int Conf on Mobile Systems, Applications, and Services. New York: ACM, 2013: 27-40

[9] Wang Xiumin, Wu Weiwei, Qi Deyu. Mobility-aware participant recruitment for vehicle-based mobile crowdsensing [J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4415-4426

[10] Chen Xi, Wu Xiaopei, Li Xiangyang, et al. Privacy-preserving high-quality map generation with participatory sensing [C] //Proc of IEEE INFOCOM 2014-IEEE Conf on Computer Communications. Piscataway, NJ: IEEE, 2014: 2310-2318

[11] Ma Rong, Chen Xiuhua, Liu Hui, et al. Research on user privacy measurement and privacy protection in mobile crowdsensing [J]. Netinfo Security, 2018, 18(8): 64-72 (in Chinese)
(马蓉, 陈秀华, 刘慧, 等. 移动群智感知中用户隐私度量与隐私保护研究[J]. 信息网络安全, 2018, 18(8): 64-72)

[12] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography [C] //Proc of EUROCRYPT'98. Berlin: Springer, 1998: 127-144

[13] Green M, Ateniese G. Identity-based proxy re-encryption [C] //Proc of the 5th Int Conf on Applied Cryptography and Network Security. Berlin: Springer, 2007: 288-306

[14] Kirtane V, Rangan C P. RSA-TBOS signcryption with proxy re-encryption [C] //Proc of the 8th ACM Workshop on Digital Rights Management. New York: ACM, 2008: 59-66

[15] Malone-Lee J, Mao W. Two birds one stone: Signcryption using RSA [C] //Proc of Cryptographers' Track at the RSA Conference. Berlin: Springer, 2003: 211-226

[16] Chandrasekar S, Ambika K, Rangan C P. RSA-TBOS signcryption with proxy re-encryption [EB/OL]. (2008-07-26) [2019-09-01]. https://eprint.iacr.org/2008/324

[17] Wang Caifen, Cao Xiaojun. An improved signcryption with proxy re-encryption and its application [C] //Proc of the 7th Int Conf on Computational Intelligence and Security. Piscataway, NJ: IEEE, 2011: 886-890

[18] Wang Huige, Wang Caifen, Cao Hao. ID-based proxy re-signcryption scheme [C] //Proc of 2011 IEEE Int Conf on Computer Science and Automation Engineering. Piscataway, NJ: IEEE, 2011, 2: 317-321

[19] Li Fagen, Liu Bo, Hong Jiaojiao. An efficient signcryption for data access control in cloud computing [J]. Computing, 2017, 99(5): 465-479

[20] Bao Guohua, Wang Shengyu, Li Yunfa. Research on data security protection method based on privacy awareness in cloud computing [J]. Netinfo Security, 2017 (1): 84-89 (in Chinese)
(包国华, 王生玉, 李运发. 云计算中基于隐私感知的数据安全保护方法研究[J]. 信息网络安全, 2017 (1): 84-89)

[21] Li Jiguo, Yao Wei, Zhang Yichen, et al. Flexible and fine-grained attribute-based data storage in cloud computing [J]. IEEE Transactions on Services Computing, 2017, 10(5): 785-796

[22] Li Jiguo, Yao Wei, Han Jinguang, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [J]. IEEE Systems Journal, 2018, 12(2): 1767-1777

[23] Li Shundong, Dou Jiawei, Wang Daoshun. Survey on homomorphic encryption and its application to cloud security [J]. Journal of Computer Research and Development, 2015, 52(6): 1378-1388 (in Chinese)
(李顺东, 窦家维, 王道顺. 同态加密算法及其在云安全中的应用[J].计算机研究与发展, 2015, 52(6): 1378-1388)

[24] Wu Yao, Zeng Juru, Peng Hui, et al. Survey on incentive mechanisms for crowd sensing [J]. Journal of Software, 2016, 27(8): 2025-2047 (in Chinese)

(吴垚, 曾菊儒, 彭辉, 等. 群智感知激励机制研究综述[J]. 软件学报, 2016, 27(8): 2025-2047)

[25] Xiong Jinbo, Ma Rong, Niu Ben, et al. Privacy protection incentive mechanism based on user-union matching in mobile crowdsensing [J]. Journal of Computer Research and Development, 2018, 55(7): 1359-1370 (in Chinese)
(熊金波, 马蓉, 牛犇, 等. 移动群智感知中基于用户联盟匹配的隐私保护激励机制[J]. 计算机研究与发展, 2018, 55(7): 1359-1370)

[26] Liao Jingxue, Chen Fuzhen, Cheng Jiujun, et al. A privacy protection system for the community IoT innovative technology and service platform [J]. Netinfo Security, 2016 (12): 60-67 (in Chinese)
(廖竞学, 陈福臻, 程久军, 等.面向社区物联网创新服务平台的隐私保护系统[J].信息网络安全, 2016 (12): 60-67)

[27] Wang Ziyu, Liu Jianwei, Zhang Zongyang, et al. Full anonymous blockchain based on aggregate signature and confidential transaction [J]. Journal of Computer Research and Development, 2018, 55(10): 2185-2198 (in Chinese)
(王子钰, 刘建伟, 张宗洋, 等. 基于聚合签名与加密交易的全匿名区块链[J]. 计算机研究与发展, 2018, 55(10): 2185-2198)

[28] Yan Jun, Ku Shaoping, Yu Chu. Reputation model of crowdsourcing workers based on active degree [J]. Journal of Computer Applications, 2017, 37(7): 2039-2043 (in Chinese)
(严俊, 库少平, 喻楚. 基于活跃度的众包工作者信誉模型[J]. 计算机应用, 2017, 37(7): 2039-2043)

[29] Shim K-A. CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks [J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883

Lai Chengzhe, born in 1985. Associate professor. Received his PhD degree from Xidian University in 2014. His main research interests include wireless network security and privacy preservation.

Zhang Min, born in 1994. Master candidate. Her main research interests include Internet of vehicles and privacy protection in crowdsensing.

Zheng Dong, born in 1964. Professor. Received his PhD degree in communication engineering from Xidian University in 1999. His main research interests include provable security and new cryptographic technology.