计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.20200915
59(4):894-906,2022

面向自动驾驶的高效可追踪的车联网匿名通信方案

侯慧莹[1] 廉欢欢[1] 赵运磊[1,2]
[1](复旦大学计算机科学技术学院 上海 200433)
[2](综合业务网络国家重点实验室(西安电子科技大学) 西安 710071)
(860963890@qq.com)

An Efficient and Traceable Anonymous VANET Communication Scheme for Autonomous Driving

Hou Huiying[1], Lian Huanhuan[1], and Zhao Yunlei[1,2]
[1](*College of Computer Science and Technology, Fudan University, Shanghai* 200433)
[2](*State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an* 710071)

Abstract Autonomous vehicles are the result of the combination of artificial intelligence and VANET. Because the autonomous vehicle can greatly free hands and improve traffic efficiency and safety, it has attracted wide attention of industry and researchers recently. While privacy issues such as instructions and vehicle identification have seriously hindered the application of autonomous car. The direct way to solve this problem is to expand the pseudonym-based communication schemes in VANET. However, most of these schemes not only impose a large storage burden on the vehicle but also fail to fully protect the identity privacy of the vehicle from being disclosed. In this paper, we propose an efficient and traceable anonymous VANET communication scheme for autonomous driving. In this scheme, a car is denoted by a set of attributes shared by multiple cars. Because of the one-to-many relationship between the attribute set and the vehicle, the anonymity of the vehicle is naturally realized. In addition, this scheme realizes the confidentiality of instructions and malicious vehicle tracking. In this paper, authentication encryption is integrated into attribute-based encryption scheme and a signcryption scheme is designed as the underlying technology to support the proposed anonymous communication scheme. Compared with the existing attribute-based signcryption schemes, this signcryption scheme is efficient and more suitable for automatic driving scenarios. Finally, the communication scheme is proved to be safe and efficient by formal security analysis and performance evaluation.

Key words autonomous vehicles; anonymous communication; data privacy-preserving; traceability; VANET

摘 要 自动驾驶汽车是人工智能与车联网相结合的产物.近年来,因自动驾驶汽车能极大地解放双手、提高交通效率和安全使其得到了工业界和学术界的广泛关注.然而,指令消息及车辆身份的隐私泄露问题严重阻碍了自动驾驶汽车的应用落地.解决该问题的最直接的方法是扩展使用车联网中基于假名的

收稿日期:2020-11-09;**修回日期**:2021-04-21
基金项目:国家重点研发计划项目(2017YFB0802000);国家自然科学基金项目(61877011,61472084);山东省重点研发计划项目(2017CXG0701,2018CXGC0701)
This work was supported by the National Key Research and Development Program of China (2017YFB0802000), the National Natural Science Foundation of China (61877011, 61472084), and the Shandong Provincial Key Research and Development Program of China (2017CXG0701, 2018CXGC0701).
通信作者:赵运磊(ylzhao@fudan.edu.cn)

通信方案.但是,大多数此类方案不仅对车辆造成了较大的存储负担,也无法完全保护车辆身份隐私不被泄露.为此,提出了一个面向自动驾驶的高效可追踪的车联网匿名通信方案.在该方案中,车辆由一个多辆车共享的属性集合表示.由于属性集与车辆之间的一对多的关系,车辆的匿名性能自然地得到实现.该方案还能实现指令消息的保密性以及对恶意车辆的追踪.该方案在属性基加密方案中融合了认证加密,设计出了一种签密方案.该签密方案作为底层技术用来支持提出的匿名通信方案.该签密方案相较于现存的属性基签密方案是高效的,更适用于自动驾驶场景.最后,通过形式化的安全性分析和性能评估证明该通信方案是安全且高效的.

关键词 自动驾驶汽车;匿名通信;数据隐私保护;可追溯性;车联网

中图法分类号 TP393

车联网是移动自组网的一种变体,它在过去的几年里得到了广泛的研究[1-4].在自动驾驶系统中,车辆通过装备的车载单元(on board unit, OBU)定期地向附近的车辆和路侧单元(road side unit, RSU)广播周围的交通状况[5-9].附近的车辆和RSU可以根据收到的交通状况消息及时地做出反应来避免交通混乱,比如交通拥堵,交通事故等.

近年来,随着人工智能技术的迅猛发展,也给车联网带来了新的发展机遇.2020年7月27日由国家标准化管理委员会、中共中央网络安全和信息化委员会办公室、国家发展和改革委员会、中华人民共和国科学技术部、中华人民共和国工业和信息化部5部门联合发布的《国家新一代人工智能标准体系建设指南》[10]的核心内容之一就是"人工智能与车联网的结合".作为人工智能和车联网相结合的产物,自动驾驶也得到了广泛的关注.

但自动驾驶依赖于精确的位置和时间信息,这将导致严重的隐私泄露[11].这是因为攻击者可以根据这些位置和时间信息重构出车辆的行驶路径.一般情况下,车辆的驾驶员是固定的[12],攻击者根据车辆的行驶路径可以进一步获得车辆的身份和驾驶员信息,以及其他的隐私信息.为了解决上述隐私泄露问题,需要打破位置和车辆身份之间的对应关系.

一种最直接的方法是"位置模糊".但"位置模糊"会导致无法实现自动驾驶.这是因为后台人工智能算法要根据车辆传感器收集到的路况信息以及车辆的位置信息来为车辆规划出下一步的行驶路线.另一种有效的方法是在通信过程中隐藏车辆的真实身份.为了保护车辆身份的隐私性,涌现出一系列基于假名机制的车联网匿名通信方案.不过需要注意的是,1个假名是远远不够的[13].攻击者还是可以轻易地将收集到的假名的位置信息与特定的车辆联系起来.

为了解决上述问题,现存的许多匿名通信方案[14-26]都建议每辆车预先存储大量的假名,以便定期更换假名.然而,即使定期更换假名可以在一定程度上保护了车辆的行驶路径不被泄露.但攻击者仍然可以利用多重假设跟踪(multiple hypothesis tracking, MHT)技术重构出车辆行驶路径,详情见第2节.

为了保护车辆行驶路径不被泄露,研究人员提出了多种假名更换策略以降低MHT成功的概率,如设置驱动速度作为假名更换[27]的触发点,在特定区域(混合区)[28]或特定时间(沉默期)[29]更换假名.总之,假名更换越频繁,抵御MHT的效果就越好.但频繁更换假名会给资源受限的网络带来沉重的存储负担.因此,怎样设计一个面向自动驾驶的高效可追踪的车联网匿名通信方案仍需要进一步探索.

本文贡献可以归纳为3个方面:

1) 提出了一个面向自动驾驶的高效可追踪的车联网匿名通信方案.在本文方案中,车辆由1个由多辆车共享的属性集合表示.由于属性集与车辆之间的1对多的关系,车辆的匿名性能自然地得到实现.此外,在本文方案中,指令消息以密文形式进行传输,也允许可信的权威(trusted authority, TA)通过传输的指令消息对恶意的车辆进行追溯和惩罚.

2) 设计了一个高效的签密方案.本文将认证加密(authentication encryption, AE)融合到传统的属性加密方案中设计出一个签密方案.该签密方案相较于现存的属性基签密方案是高效的,更适用于自动驾驶场景.

3) 通过形式化的安全性分析和一系列仿真实验证明本文方案是安全和高效的.

1 相关工作

为了保护车辆行驶路径不被暴露,研究学者们

提出了许多基于公钥加密、身份基加密、群签名和无证书的匿名通信方案[9,14-15,17-18,30-39].然而,由于需要频繁地更新假名或私钥,上述所有方案都给车辆带来了沉重的计算和存储负担.

在基于公钥加密的方案[14-15,17]中,公共基础设施(public key infrastructure, PKI)须向车辆用户颁发公钥证书.由于需要频繁地更换假名,在基于公钥加密的方案中,每辆车都要预先存储大量的公私钥对和公钥证书,这给资源受限的车辆带来了沉重的存储负担.与基于公钥加密的方案相比,身份基的匿名通信方案[18,30]不再需要给车辆颁发公钥证书.基于身份的匿名通信方案依靠可信的权威机构来为每辆车生成假名.同时车辆也需要预先存储大量的假名.为了降低车辆的存储负担,提出了基于群签名和无证书的匿名通信方案[31-32,38-39].然而,上述提及的通信方案[14-15,17-18,31-32,38-39]方案均不能同时实现传输消息的保密性和车辆身份的隐私保护,且大部分都不支持对恶意车辆的追责.

为了同时实现车辆身份的隐私保护、传输消息的保密性以及对恶意车辆的追溯,Cui 等人[8]提出了一种基于属性的动态属性通信框架.但是,在该方案中,车辆的密钥长度太长且计算开销大.具体地,车辆的密钥长度与$|W|\cdot|Path(x)|$成正比,其中$|W|$表示为车辆拥有的属性集合 W 包含的属性的个数,$|Path(x)|$表示代表车辆的叶子结点 x 到二叉树根结点路径 $Path(x)$包含的结点个数.文献[8]中的方案给车辆造成了较大的存储负担,如何设计一个面向自动驾驶的高效可追踪的车联网匿名通信方案是十分有意义的.

2 背景知识

1) 双线性映射

设 G_1,G_2,G_T 为 3 个大素数 p 阶的乘法循环群.g_1,g_2 分别是群 G_1,G_2 的生成元.双线性映射是一个具有 3 个特点的映射 $e:G_1\times G_2\rightarrow G_T$:

① 双线性.对任意的 $g_1\in G_1,g_2\in G_1$ 以及 $a,b\in\mathbb{Z}_p^*$,$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$.

② 非退化性.g_1 和 g_2 分别是群 G_1 和 G_2 的生成元,$e(g_1,g_2)\neq 1$.

③ 可计算性.对所有的 $g_1\in G_1,g_2\in G_2$,$e(g_1,g_2)$都是可以高效计算的.

设 G_1,G_T 为 2 个大素数 p 阶的乘法循环群,g_1 为群 G_1 的生成元,那么 $e:G_1\times G_1\rightarrow G_T$ 为双线性映射.

2) 离散对数问题

离散对数问题指的是,给定素数 p 阶循环群 G_1 的生成元 g,$g^x\in G_1,x\in\mathbb{Z}_p^*$,计算 x.

3) 双线性 Diffie-Hellman 判定问题

双线性 Diffie-Hellman 判定问题指的是,给定$(g_1,g_1^a,g_1^b,g_1^c)\in G_1^4$ 和 $\mu\in G_T$,判定 μ 是否等于 $e(g_1,g_1)^{abc}$.

4) 认证加密

简而言之,在认证加密方案中,密文 C 不仅包含有加密后的消息 M 也包含有关联数据 H(例如 1 个数据包或 1 个 IP 地址)[40].关联数据 H 是用于验证的,它的内容一般由上下文来决定.

5) 访问控制树

在访问控制树中,可以使用 1 组描述性属性对密文进行标记.访问控制树的结构可以确定解密密文的私钥集合.每棵树的内部结点是 1 个阈值门,叶子与属性相关联.只有当分配给树结点的密文属性与要求一致时,用户才能用给定的密钥解密相应的密文.

1 个访问控制树的每个非叶子结点代表 1 个阈值门,由其子结点和 1 个阈值描述.num_x 表示结点 x 的孩子数,v_x 为该结点的阈值,其中 $0<v_x\leqslant num_x$.当 $v_x=1$ 时,阈值门为 OR 门;当 $v_x=num_x$ 时,阈值门为 AND 门.访问控制树的每个叶子结点 x 代表 1 个属性且它的阈值 $v_x=1$.在本文中,如果 x 为非叶子结点,那么阈值门为 AND 门.

为了使访问控制树更加方便实用,定义了一些函数.定义 $parent(x)$表示为结点 x 的父结点.当 x 为叶子结点时,$att(x)$表示为其代表的属性.访问控制树中也定义了结点 x 的孩子们的顺序,从 1 到 num_x.$index(x)$为结点 x 为其父结点的第 x 个孩子.

令访问控制树 Γ 的根结点为 r.Γ_x 表示为其根结点为 x 的 Γ 的子树.如果属性集合 W 满足访问控制树 Γ_x,则 $\Gamma_x(W)=1$.$\Gamma_x(W)$的计算方式为:如果 x 为非叶子结点,计算其所有孩子 x'的 $\Gamma_{x'}(W)$,至少 v_x 个孩子结点返回 1 时,$\Gamma_x(W)$才等于 1;如果 x 为叶子结点,只有当 $att(x)\in W$ 时,$\Gamma_x(W)$才等于 1.

6) 多重假设跟踪(MHT)

如图 1 所示,多重假设跟踪技术可以根据一段时间内的确定轨迹猜测出用户更长一段时间内的行驶路径.例如,我们现在知道了假名一段时间内的确定轨迹(1,2).根据确定的轨迹,MHT 通过卡尔曼滤波器来预测下一假名时间段内的位置(3)[13].然

后,MHT 接收到 2 个测量值 A 和 B,它们可以与现有的轨迹相关联,也可以作为新轨迹的起点.根据 MHT 理论,每条假设路径都用概率进行了标记.如图 1(a)所示,最有可能的关联值是 $B=3$,因为 B 比 A 更接近估计位置 3.接下来,MHT 分别基于优先路径 A 和(1,2,B)估计位置 2 和 4.在接收到 2 个新的测量值后,MHT 计算每个假设的概率.如图 1(b)所示,D 既不接近 4 也不接近 2,得到的 P_{21} 和 P_{22} 会很小.因此,当考虑这 2 个步骤时,如图 1(c)所示,假设路径(1,2,A,C)是车辆最可能行驶的路径.

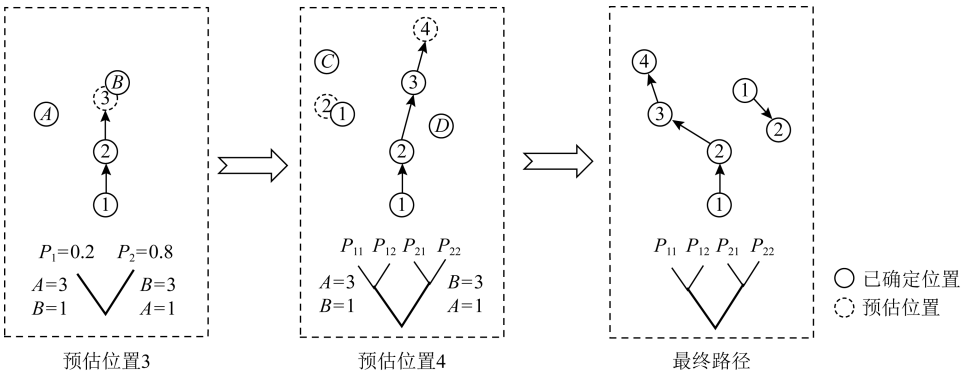

Fig.1 The example of MHT

图 1 MHT 示例

3 系统模型和安全模型

3.1 系统模型

如图 2 所示,本文的系统模型包含了 4 种不同的实体:可信的权威(TA)、交通控制中心、路侧单元(RSU)以及车载单元(OBU).

1) 可信权威(TA).TA 是一个具有大量计算资源的可信第三方.实际上,自动驾驶是一种按需服务的交通服务系统.该服务提供方就可作为系统模型中的 TA,它只为订购自动驾驶的用户提供服务.当 RSU 和 OBU 想要加入到自动驾驶系统时,TA 为其提供离线的注册服务.注册完成后,RSU 和 OBU 可以将系统参数和密钥通过离线的方式预下载到本地.根据 OBU 和 RSU 的要求,TA 还可提供其他一些服务.所有车辆进入系统前必须通过离线的方式向 TA 登记详细的身份信息.在系统中,车辆需要直接向 TA 中提供必要的信息,如姓名、电话、地址等.在本文的系统模型中,TA 还作为一个仲裁机构,是唯一可以在传输的消息中提取发送方身份信息的实体.

2) 交通控制中心.交通控制中心是一个具有丰富计算资源并拥有人工智能算法的实体.在自动驾驶

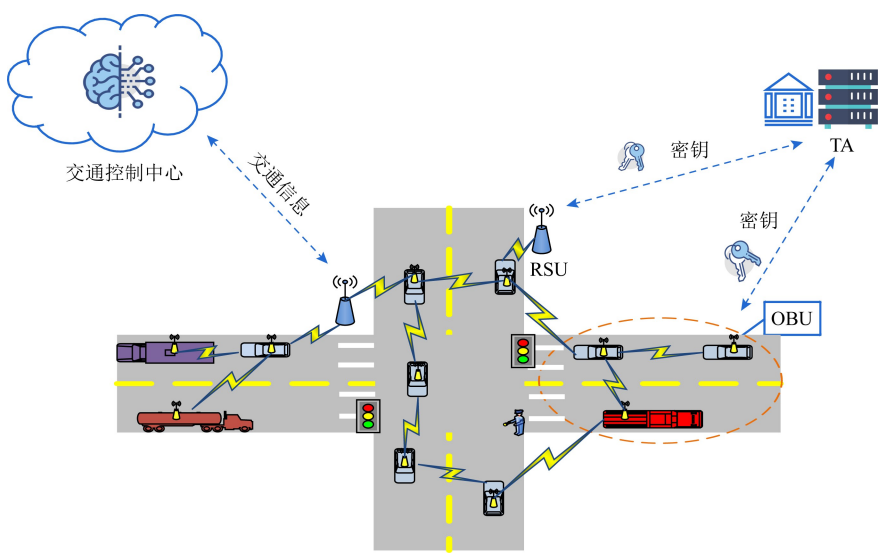

Fig. 2 The system model of this paper

图 2 本文的系统模型

系统中,交通控制中心可以根据车辆搜集到的交通状况信息通过人工智能算法为用户规划下一步的行驶路线.

3) 路侧单元(RSU).RSU 通过无线信道与被覆盖区域内的车辆以及其他的 RSU 进行通信.RSU 是半可信的.当 RSU 受到攻击时,它可以向对手泄露机密数据.为了防止硬件发生故障,所有 RSU 都应该受到监视,比如闭路电视或摄像机.

4) 车载单元(OBU).每辆车上都装备有车载单元 OBU.车辆通过自身装备的 OBU 与其他车辆和 RSU 的通信.通过定期广播交通状况,比如位置、速度和紧急事件,OBU 可以帮助其他车辆改变它们的运动轨迹来避免交通拥堵或交通事故.

3.2 设计目标

一个安全的面向自动驾驶的高效可追踪的车联网匿名通信方案应该满足 5 个要求:

1) 机密性.只有属性集合满足密文访问控制结构的车辆才能对密文进行正确的解密.

2) 匿名性.接收者不知道哪辆车发送的消息.有且只有 TA 能追踪到消息的发送方.

3) 可追溯性.在车联网中,TA 可以准确地捕获信息的发送者,并对恶意车辆进行惩罚.

4) 抗多重假设跟踪.敌手无法通过使用 MHT 技术来重构出车辆的行驶路径.

5) 抗假冒攻击.一个有效的接收者不能假装成另一接收者与其他车辆通信.

3.3 定 义

定义 1. 一个面向自动驾驶的高效可追踪的车联网匿名通信方案由 6 种算法组成:Join, Setup, KeyGen, TransMessage-Generation, Message-Verification, Tracking.这些算法的详细定义为:

$Join(name, address, mobilenumber)\rightarrow(rid, pwd)$.该算法由 TA 执行.它以车辆用户的姓名、地址和手机号码作为输入.然后,输出车辆的真实身份 rid 和相关的 OBU 的访问密码 pwd.

$Setup(1^k)\rightarrow(par, msk)$.该算法由 TA 执行.它以安全参数 k 为输入,输出系统的公开参数和主私钥 msk.

$TransMessage\text{-}Generation(par, W, sk_s, H, M)\rightarrow C$ 或 $\perp$.这是一个概率算法.它以系统的公开参数 par、发送者的私钥 sk_s、消息 M、属性集合 W 以及关联数据 H 为输入,其输出传输消息的密文 C 或者 $\perp$.$\perp$ 代表程序运行失败.

$KeyGen(par, msk)\rightarrow sk$.该算法由 TA 执行.它以系统的公开参数 par、主私钥 msk 为输入,其输出用户的私钥 sk.

$Message\text{-}Verification(par, C)\rightarrow M$ 或 $\perp$.这是一个确定性的算法.它以系统的公开参数 par 和密文 C 为输入.如果通过了验证算法,该算法输出消息 M,否则输出 $\perp$.

$Tracking(id, msk)\rightarrow rid$.该算法由 TA 执行.它以 $id=rid^{msk}$ 以及主私钥 msk 为输入,而后输出发送者的真实身份 rid.

3.4 安全模型

为了形式化描述本方案安全模型,我们引入了挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 之间的游戏.通过该游戏来说明敌手 $\mathcal{A}$ 是如何攻破自动驾驶通信方案的安全性.在本文的安全模型中,TA 被视为挑战者 $\mathcal{C}$,而恶意的接收方被视为敌手 $\mathcal{A}$.

1) Setup 阶段.敌手 $\mathcal{A}$ 将想要挑战的属性集 W 发送给挑战者 $\mathcal{C}$.而后,挑战者 $\mathcal{C}$ 运行 Setup 算法并将公开参数 par 发送给敌手 $\mathcal{A}$.

2) KeyGen 询问阶段.在这个阶段,敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{C}$ 发送多项式次私钥问询.挑战者 $\mathcal{C}$ 运行 KeyGen 算法为访问控制结构 Γ_j ($W\notin\Gamma_j$) 生成私钥,并将其发送给敌手 $\mathcal{A}$.

3) Challenge 阶段.在此阶段,敌手 $\mathcal{A}$ 随机选择 2 个长度相同的消息 M_0 和 M_1,并将这 2 个消息发送给挑战者 $\mathcal{C}$.而后,$\mathcal{C}$ 随机选择 $b\leftarrow\{0,1\}$,并运行 TransMessage-Generation 算法在属性集为 W 下为消息 M_b 生成密文 C.最后,挑战者 $\mathcal{C}$ 将密文发送给敌手 $\mathcal{A}$.

4) Guess 阶段.敌手 $\mathcal{A}$ 首先执行与 KeyGen 询问阶段同样的操作.而后,敌手 $\mathcal{A}$ 输出 b'.

在上述安全模型中,需要证明如果拥有属性集的敌手 $\mathcal{A}$ 不符合密文的访问控制结构,就无法正确解密密文.敌手 $\mathcal{A}$ 的目标是正确猜测出挑战者 $\mathcal{C}$ 生成的挑战密文 C 中的加密消息 M_b.

把该游戏中敌手 $\mathcal{A}$ 胜出的概率定义为

$$Pr[b'=b]-\frac{1}{2}.$$

定义 2. 如果在选择集合安全模型下所有的多项式时间敌手获得胜利的概率均是可以忽略的,那么本文中面向自动驾驶的高效可追踪的车联网匿名通信方案是安全的.

本文认为接收者不是完全可信的.满足访问控制结构的接收方可能希望在下一次与其他车辆的通信

中假冒此次通信的发送方.因此,密文中包含的发送者身份信息应该是一次性的.也就是说,即使有效的接收方知道发送方的身份信息,也不能冒充发送方与其他车辆或 RSU 进行通信.考虑到上述情况,给出了下面的安全定义.

定义 3. 如果任何有效的接收方都不能伪装成相应的接收方与其他车辆进行下一次通信,那么我们可以说本文提出的面向自动驾驶的高效可追踪的车联网匿名通信方案是可以抵御假冒攻击.

4 本文方案

在实际应用中,可以使用 1 组属性集合{省,市,街道,RSU},{市,街道,RSU}或者{街道,RSU}来代表车辆或 RSU,相应的 TA 分别管理 1 个国家、1 个省或者 1 个直辖市.在本文方案中,TA 管理 1 个国家.为了将每一个属性映射到$\mathbb{Z}_p^*$中 1 个元素,本文对所有属性进行了编号.一般情况下,1 个国家的省或直辖市的数量和每个城市的区或县的数量变化很小.为了将属性集合映射到$\mathbb{Z}_p^*$,可以按照省、市、街道、RSU 的顺序进行连续编号.为了可以支持省、市、街道、RSU 数量的变化,每部分可以酌情预留出一些元素.例如,n_1-24 为上海市区或县的数量与为区属性预留出来的元素个数的总和,n_2-n_1-1 表示为上海市杨浦区的街道个数与为街道属性预留出来的元素个数的总和.TA 负责治理 1 个国家,而后对全国所有省份进行编号,如上海为 1、山东为 2、河南为 3 等.进一步,可以对这个省的所有城市、街道和 RSU 进行编号.例如,属性集合{上海,杨浦,邯郸,RSU_1}可以表示为 $W=\{1,24,n_1+1,n_2+1\}$.

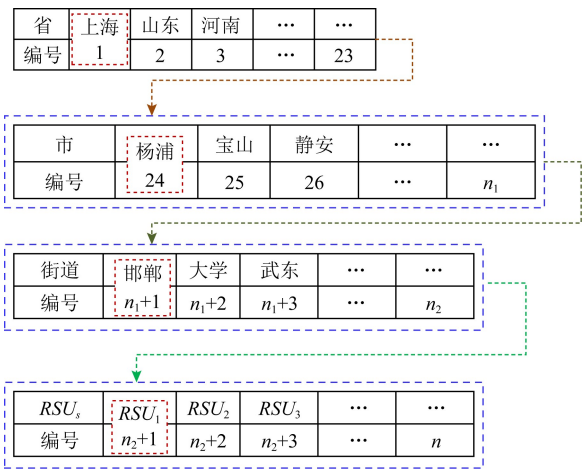

Fig.3 The number of attributes

图 3 属性的编号方式

为了实现可追溯性,密文应该包含发送者身份的相关信息,只有 TA 可以根据这些相关信息跟踪发送者的身份.此外,车联网要求极高的实时性,密文应包含时间信息,以防止重放攻击.

本文详细描述了提出的抗 MHT 车辆网匿名通信方案的 6 种算法.

1) $Join(name,address,mobilenumber)$.当车辆首次加入系统时,它首先离线地向 TA 完成注册.注册时,车辆拥有者需要向 TA 提交一些必需的信息,如姓名、车牌号、地址以及手机号.注册成功后,TA 为该车辆颁发 1 个唯一的车辆表示 RID 以及车载单元的访问口令 pwd.在这里,OBU 是车辆的防篡改设备,如果用户想访问它的 rid,他需要使用相关的 OBU 的访问口令 pwd.

2) $Setup(1^k)$.假设所有省、市、街道以及 RSU 的总数量为 n.而后,本文使用$\mathbb{Z}_p^*$中前 n 个元素代表属性集合,也就是属性集合可以表示为 $U=\{1,2,\cdots,n\}$.而后,为每个 $i\in U$ 选择 1 个随机数 $t_i\in\mathbb{Z}_p$.最后,选择随机数 $y_1\leftarrow\mathbb{Z}_p$,$y_2\leftarrow\mathbb{Z}_p^*$并计算 $Y=g_1^{y_1}$,$id=(rid)^{y_2}$.最后,TA 将 id 通过安全信道发送给车辆.

公开的系统参数为 $par=\{T_1=g_1^{t_1},T_2=g_1^{t_2},\cdots,T_n=g_1^{t_n};Y=g_1^{y_1}\}$.

主私钥为 $msk=\{t_1,t_2,\cdots,t_n;y_1,y_2\}$.

3) $TransMessage\text{-}Generation(par,W,id,H,M)$.令 $SE=(K_{SE},Enc,Dec)$为认证加密算法.$M\in\{0,1\}^*$为消息,$H\in\{0,1\}^*$为关联数据,$W\subseteq U$为属性集合.$KDF:G_T\times G_T\rightarrow\{0,1\}^*$表示为密钥推导函数,在实际中可以视为一个随机预言机.

为了传输消息 $M\in\{0,1\}^*$,发送者进行 5 个操作:

① 选择随机数 $x\leftarrow\mathbb{Z}_p^*$,并生成 $X=\{T_i^x\}_{i\in W}$;

② 计算预共享密钥 $PS=e(g_1,Y)^x$;

③ 计算密钥 $k_1=KDF(X,PS)$;

④ 计算 $C_{AE}\leftarrow Enc_{k_1}(H,M\parallel id\parallel T_i)$,其中 $id=(rid)^{y_2}$,T_i 为时间戳.

⑤ 广播传输消息 $C=(H,X,C_{AE})$.

4) $KeyGen(par,msk)$.TA 为拥有属性集合为 W 的接收者生成解密密钥 D.当且仅当 $\Gamma(W)=1$ 时,拥有解密密钥 D 的接收者可以解密密文 C.TA 进行 2 个操作:

① 以从上到下的方式,从根结点 r 开始为访问控制树 Γ 中的每个结点 w 选择一个多项式 q_w.每个结点 w 的多项式 q_w 的秩为 $d_w=v_w-1$,这里的 v_w

为该结点的阈值.对于根结点 r,令 $q_r(0)=y$,对多项式 q_r 的其他 d_r 点进行随机定义.对于树中的其他结点 w,令 $q_w(0)=q_{parent(w)}(index(w))$,多项式中的其他点也是随机进行定义.

② 对于每个叶子结点,将下面的秘密值发送给接收者:

$$D_w=g_1^{\frac{q_w(0)}{t_i}},$$

其中,$i=att(x)$.

解密密钥 D 为所有这些秘密值的集合.

5) *Message-Verification*(par,C).当收到密文 $C=(H,X,C_{AE})$后,接收者向 TA 发送解密密钥请求.收到请求后,TA 进行 3 个操作.

① 定义 1 个递归算法 *DecryptNode*(D,w)来计算 PS.当 w 为叶子结点时,算法为每个 $i\in W$ 计算 $DecryptNode(D,w)=e(T_i^x,D_w)$.如果 $i\notin W$,算法返回 $\perp$.当 w 为非叶子结点时,算法运行如下:对于所有 w 的孩子结点 z,算法调用 *DecryptNode*(D,z),并将该结果存储为 F_z.令 S_z 为任意 D_w 大小的满足 $F_z\neq\perp$的孩子结点的集合.如果不存在这样的集合,那么算法返回 $\perp$.否则,计算

$$F_w=\prod_{z\in S_w}F_z^{\Delta_{i,S'_w(0)}}=$$

$$\prod_{z\in S_w}(e(g_1,g_1)^{x\cdot q_z(0)})^{\Delta_{i,S'_w(0)}}=$$

$$\prod_{z\in S_w}(e(g_1,g_1)^{x\cdot q_{parent(z)}(index(z))})^{\Delta_{i,S'_w(0)}}=$$

$$\prod_{z\in S_w}(e(g_1,g_1)^{x\cdot q_w(i)})^{\Delta_{i,S'_w(0)}}=e(g_1,g_1)^{s\cdot q_w(0)}.$$

这里 $i=index(z)$,$S'_w=\{index(z):z\in S_w\}$.最后返回该计算结果.

为了计算预共享的 PS,在树根上调用该算法.可以得到 $DecryptNode(D,r)=e(g_1,g_1^y)^x=PS$.

② 获得 PS 之后,计算密钥 $k_1=KDF(X,PS)$.

③ 计算 $H,M,id,T_i\leftarrow Dec_{k_1}(H,M\parallel id\parallel T_i)$.

解密后,接收者首先验证解密得到的关联数据 H 是否与明文发送的关联数据相同.如果相同,再验证时间戳 T_i 是否与系统时间相吻合,如果是,接收消息 M 并保存 id.否则,返回 $\perp$.

6) *Tracking*(id,msk).当 TA 需要追溯消息的发送者时,它可以通过 2 种方式来获得车辆的 rid.其中一种是通过解密密钥 D 解密密文 C,得到 $id=(rid)^{y_2}$,而后用主密钥 y_2 得到 rid.另一种方法是接收者向 TA 发送追溯请求,而后将 $id=(rid)^{y_2}$ 发送给 TA.而后用主密钥 y_2 得到 rid.TA 追溯到恶意发送者后对其进行惩罚.

5 安全性分析

本节通过机密性、匿名性、可追溯性、抗多重假设跟踪、抗假冒攻击 5 个方面证明本文方案是安全的.

定理 1. 机密性.假设在双线性群中 DBDH 问题是困难的,并且用于生成密文的认证加密是安全的.在该方案中,对于不拥有符合密文访问控制结构的属性集的敌手,是不能解密密文的.

证明. 为了证明该定理,定义了一个敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏.

游戏 1. 在游戏 1 中,敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 执行如安全模型中一样的操作.也就是,挑战者 $\mathcal{C}$ 运行 Setup 算法生成主私钥 msk 以及系统的公开参数 par.而后,$\mathcal{C}$ 将公开参数 par 发送给 $\mathcal{A}$.接下来,挑战者 $\mathcal{C}$ 运行 KeyGen 算法为 $W(W\notin\Gamma_j)$生成私钥.敌手 $\mathcal{A}$ 随机选择 2 个长度相同的消息 M_0 和 M_1,并将发送给挑战者 $\mathcal{C}$.而后,$\mathcal{C}$ 随机选择 $b\leftarrow\{0,1\}$,并运行 TransMessage-Generation 算法在属性集为 W 下为消息 M_b 生成密文 C.最后敌手 $\mathcal{A}$ 输出 b'.

假设敌手能够以不可忽略的概率在游戏 1 中获得胜利.基于此,可以构造出一个模拟器 $\mathcal{B}$ 来解决 DBDH 问题.给定 2 组参数$(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^{abc})(\mu=0)$和$(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^z)(\mu=1)$,其中 $a,b,c,z\leftarrow\mathbb{Z}_p^*$,模拟器 $\mathcal{B}$ 的目标是输出 μ.而后,$\mathcal{B}$ 做游戏 1 中挑战者 $\mathcal{C}$ 的操作.

1) Setup.挑战的属性集合为 W.模拟器 $\mathcal{B}$ 设置 $Y=g^{ab}$.对所有的 $i\in W$,模拟器 $\mathcal{B}$ 设置 $T_i=g^{r_i}(t_i=r_i)$,其中 $r_i\in_R\mathbb{Z}_p$.对 $i\notin W$,设置 $T_i=g^{b\beta_i}=B^{\beta_i}(t_i=b\beta_i)$,其中 $\beta_i\in_R\mathbb{Z}_p$.然后,模拟器 $\mathcal{B}$ 将这些公开参数发送给敌手 $\mathcal{A}$.

2) KeyGen 询问阶段.对于满足 $\Gamma(W)=0$ 的访问控制结构,敌手 $\mathcal{A}$ 可以自适应地进行相关密钥的问询.为了产生相关的私钥,对访问控制结构 Γ 中的每一个结点,模拟器 $\mathcal{B}$ 均为其选择一个秩为 d_x 的多项式 Q_x.

下面定义了 2 种程序 PolySat 和 PolyUnsat.

PolySat(Γ_x,W,λ_x).该算法的目标是为满足 $\Gamma_x(W)=1$ 的结点选择多项式.该算法的目标是以访问控制树 Γ_x、属性集合 W 以及整数 $\lambda_x\in\mathbb{Z}_p$ 作为输入.首先,对于根结点 x,为其分配一个阶为 d_x 的多项式 q_x,令 $q_x(0)=\lambda_x$.并随机地定义多项式总的

其他点以固定多项式 q_x.而后,调用 $PolySat(\Gamma'_x, W, q_x(index(x')))$为结点 x 的每个子结点 x'分配多项式,令 $q_{x'}(0)=q_x(index(x'))$.

$PolyUnsat(\Gamma_x, W, g^{\lambda_x})$.该算法的目标是为满足 $\Gamma_x(W)=0$ 的结点选择多项式.该算法的目标是以访问控制树 Γ_x、属性集合 W 以及整数 $g^{\lambda_x}\in G_1$ 作为输入.首先,对于根结点 x,为其分配一个阶为 d_x 的多项式 q_x,令 $q_x(0)=\lambda_x$.由于 $\Gamma_x(W)=0$,小于 d_x 个 x 的孩子可以满足要求.假设 $h_x\leqslant d_x$ 为结点 x 的孩子数.为每个孩子结点 x'设置 $q_x(index(x'))=\lambda_{x'}$.

为了计算该算法其他结点的多项式,对每个结点 x 的子结点 x',调用算法:

① $PolySat(\Gamma_{x'}, W, q_x(index(x')))$.如果 x'为内部结点,$q_x(index(x'))$是已知的.

② $PolyUnsat(\Gamma_{x'}, W, g^{q_x(index(x'))})$.如果 x'为非内部结点,那么只有在差值 $g^{q_x(0)}$ 已知的情况下才能获得 $g^{q_x(index(x'))}$.

在这种情况下,结点 x 的每个孩子结点都有 $q_{x'}(0)=q_x(index(x'))$.

为了生成满足访问控制结构 Γ 的密钥,模拟器 $\mathcal{B}$ 首先调用 $PolyUnsat(\Gamma, W, A)$为树中的每一个结点分配一个多项式 q_x.对每个叶子结点,如果 x 是内容结点可以得到 q_x,如果不是,可以得到 $g^{q_x(0)}$.进一步得到 $q_r(0)=a$.

目前,模拟器 $\mathcal{B}$ 可以为每个结点 x 总结出最后的多项式 $Q_x(\cdot)=bq_x(\cdot)$.也应该考虑到 $y=Q_r(0)=g^{ab}$.叶子结点的密钥计算为

$$D_x=\begin{cases} g^{\frac{Q_x(0)}{t_i}}=g^{\frac{bq_x(0)}{r_i}}=B^{\frac{q_x(0)}{r_i}}, & \text{若 } att(x)\in W,\\ g^{\frac{Q_x(0)}{t_i}}=g^{\frac{bq_x(0)}{b\beta_i}}=B^{\frac{q_x(0)}{\beta_i}}, & \text{其他.}\end{cases}$$

最后,模拟器 $\mathcal{B}$ 可以为访问控制结构 Γ 产生密钥.最重要的是,这样产生的密钥与原始算法相同.

3) Challenge 阶段.敌手 $\mathcal{A}$ 随机选择 2 个长度相同的消息 M_0 和 M_1,并将这 2 个消息发送给模拟器 $\mathcal{B}$.而后,模拟器 $\mathcal{B}$ 随机选择一个比特随机数 θ,并将 M_θ 的密文发送给敌手 $\mathcal{A}$.$\mathcal{B}$ 通过以下方式得到 PS:

$$Z=PS=(g,Y)^x=(g,g^{ab})^x.$$

如果 $\mu=0$,那么 $Z=e(g,g)^{ab}$.如果令 $x=c$,可以得到 $Z=PS=(g,g)^{abc}$.如果 $\mu=1$,$Z=e(g,g)^z$.

而后可以得到密钥 $k_1=KDF(T_i^x,Z)$,并输出密文 $C_{AE}\leftarrow Enc_{k_1}(H, M_\theta \parallel id \parallel T_i)$.由于散列函数 KDF 和认证加密的安全性,要破解加密算法,必须先获得 PS.

4) Guess 阶段.敌手 $\mathcal{A}$ 首先执行与 KeyGen 询问阶段同样的操作.而后,$\mathcal{A}$ 输出比特 θ'.如果 $\theta'=\theta$,则敌手获得胜利.

从上述 4 个阶段中可以看出,参数和私钥的生成都与真正的方案相同.

假设 $\mu=1$,敌手 $\mathcal{A}$ 等不到关于 θ 的任何有用信息.因此我们得到 $Pr[\theta'\neq\theta|\mu=1]=\frac{1}{2}$.因为模拟器 $\mathcal{B}$ 在 $\theta'\neq\theta$ 情况下猜测 $\mu'=1$,故可以得到 $Pr[\mu=\mu'|\mu=1]=\frac{1}{2}$.

假设 $\mu=0$,定义敌手 $\mathcal{A}$ 成功的概率为 ε.也就是敌手 $\mathcal{A}$ 可以以概率 ε 计算出 PS.因此有 $Pr[\theta'\neq\theta|\mu=0]=\frac{1}{2}+\varepsilon$.因为模拟器 $\mathcal{B}$ 在 $\theta'=\theta$ 情况下猜测 $\mu'=0$,故可以得到 $Pr[\mu=\mu'|\mu=0]=\frac{1}{2}+\varepsilon$.

模拟器 $\mathcal{B}$ 解决 DBDH 问题的概率为 $\frac{1}{2}Pr[\mu=\mu'|\mu=0]+\frac{1}{2}Pr[\mu=\mu'|\mu=1]-\frac{1}{2}=\frac{1}{2}(\frac{1}{2}+\varepsilon)+\frac{1}{2}\times\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$.因此,如果敌手 $\mathcal{A}$ 能以概率 ε 成功攻破本文提出的方案,模拟器 $\mathcal{B}$ 就能以不可忽略的概率 $\frac{1}{2}\varepsilon$ 解决 DBDH 问题. 证毕.

定理 2. 匿名性.除了 TA,没有人可以知道消息发送者的真实身份.

证明. 在该方案中,每辆车由多辆车共享的一个属性集表示.此外,在方案执行过程中,参数 $X=\{T_i^x\}_{i\in W}$ 以及 $PS=e(g_1,Y)^x$ 都不包含发送车辆的真实身份信息.只有当加密过程时,才会包含用主密钥 y_2 加密的身份信息 $id=(rid)^{y_2}$.根据 AEAD 方案的安全性,外部对手无法获取明文信息.因此,外部敌手不能获得关于车辆身份 rid 的任何信息.即使接收者得到了 $id=(rid)^{y_2}$,也无法知道 rid 除非它能解决离散对数问题.因此,本文提出的抗 MHT 的车联网匿名安全通信方案实现了车辆的匿名性. 证毕.

定理 3. 可追溯性.该方案允许 TA 追溯到恶意的发送者并对其进行惩罚.

证明. 车辆的真实身份包含在 $id=(rid)^{y_2}$ 中,TA 可以通过使用拥有的主私钥 y_2 得到 rid.因此,本文提出的抗 MHT 的车联网匿名安全通信方案实现了对恶意车辆的可追溯性. 证毕.

定理 4. 抗多重假设跟踪.在本文方案中,对手不能利用 MHT 技术重构出车辆的行驶路径.

证明. 在本文方案中,每辆车都用 1 个由多辆车共享的属性集来表示.因此,即使在同一区域,也可能有多个车辆具有同一属性集.在这种情况下,对手无法在短时间内得到确定的路径作为 MHT 算法的输入,使得敌手无法运行 MHT 算法来重构车辆的路径.因此,本文提出的抗 MHT 的车联网匿名安全通信方案抗多重假设跟踪. 证毕.

定理 5. 抗假冒攻击.没有一辆车能假冒另一辆合法车来给进行通信.

证明. 为了假冒成其他的车辆或者 RSU,敌手必需产生合法的密文 $C=(H,X,C_{AE})$,其中 $C_{AE}\leftarrow Enc_{k_1}(H,M\|id\|T_i)$.该 id 是由 TA 根据车辆的真实身份 rid 生成的,每次信息传输时,id 值是不同的.因此,对手不能伪造出合理的密文.总体而言,本文提出的抗 MHT 的车联网匿名安全通信方案能够抵御假冒攻击. 证毕.

6 性能评估

本节首先对本文提出的方案进行了定性评估.而后,将本文方案与最近提出的方案[23,25-26,41]进行了功能性的对比.最后通过一系列仿真实验验证了该方案的有效性.

本文用到的双线性映射定义为 $e:G_1\times G_1\rightarrow G_T$.为了方便表示,定义以下符号来表示方案中的操作:令 $Hash$,$Exp(G_1)$和 $Mul(G_1)$分别表示一个散列操作、一个群 G_1 中的模幂操作和一个群 G_1 中的模乘操作.同样地,$Exp(G_T)$和 $Mul(G_T)$分别表示一个群 G_T 中的模幂操作和一个群 G_T 中的模乘操作.$Pair$ 表示为一次双线性映射操作.令属性集合为 W,$|W|$表示属性集合中包含的属性个数.令 Enc 和 Dec 分别表示认证加密中的加密和解密操作.

1) 性能分析

如表 1 所示,在本文方案中,发送者首先要为每个属性计算 $X=\{T_i^x\}_{i\in W}$,而后发送者需要一次双线性映射操作、一次群 G_T 中的模幂操作和一次群 G_T 中的模乘操作来计算 $PS=e(g_1,Y)^x$.接下来,发送者使用散列函数 KDF 来获得加密密钥.最后,使用认证加密算法来生成密文 C_{AE}.总结起来,发送者需要执行的操作总和为 $|W|Exp_{G_1}+Pair+Exp_{G_T}+Hash+Enc$.对于接收者,它首先需要调用递归函数 $DecryptNode(D,r)$.而后,接收者可以通过 KDF 函数得到加密密钥,并使用认证加密的解密算法得到明文 M.因此,接收者需要执行的操作总和为 $\left(\sum_{i=0}^{2^{\lceil \lg|W| \rceil}}2^i\right)\times Mul_{G_1}+Pair+Hash+Dec$.

Table 1 Performance Analysis of the Proposed Scheme

表 1 本文方案的性能分析

计算者	本文方案
发送者	$\|W\|Exp_{G_1}+Pair+Exp_{G_T}+Hash+Enc$
接收者	$\left(\sum_{i=0}^{2^{\lceil \lg\|W\| \rceil}}2^i\right)\times Mul_{G_1}+Pair+Hash+Dec$

2) 功能对比

将本文的方案与 9 个相关文献[8-9,23,25-26,33-35,41]进行了功能对比.如表 2 所示,文献[33-35]不满足匿名性.也就是,在文献[33-35]中,车辆在通信中不能够隐藏真实身份,这严重侵犯了车辆的身份隐私.文献[25-26]不能抵御假冒攻击.也就是,在文献[25-26]中,一个恶意的敌手可以伪装成另一辆合法车辆与其他车辆进行通信.文献[23,25-26]不能抵御篡改攻击,恶意的敌手可以通过篡改传输中的交通状况信息来制造交通事故.文献[8-9,33-35]不能抵御重放攻击.一个恶意的接收方,可以冒充成之前与其通信的发送方车辆向其他车辆发送之前它接收到的消息.文献[23,25-26,33-35,41]不能保证传输消息的机密性.文献[25-26]不能实现可追溯性,无法完成对恶意车辆的追责.文献[9,23,25-26,33-35,41]均不能抵御 MHT.敌手可以使用 MHT 技术完成对文献[9,23,25-26,33-35,41]中车辆行驶路径的重构.总的来说,本文的方案是唯一能够满足匿名性、抗假冒攻击、篡改攻击和重放攻击、可追溯性、机密性和抗 MHT 的方案.

3) 实验结果

本节首先评估了本文方案在普通消息数量和大量消息数量这 2 种不同场景下的性能.我们设定普通消息数量在 0～100 之间,大量消息数量在 1～1 000 之间.之后,我们将结果与现存的先进的文献[8-9,33-35]进行比较.

在本节中,我们通过实验来评估本文方案的性能.仿真实验代码是使用 C++编写的,运行在 Intel 处理器为 2.30 GHz 和 8 GB 内存的 Linux 服务器上.这些实验是在基于配对的密码学库[42](版本为 PBC 0.5.14)和 GNU 多精度算法[43]的帮助下完成的.在实验中,我们使用 PBC 中的参数 $a.param$ 来设置基础字段大小为 320 KB,分为 16 384 块,$\mathbb{Z}_p$ 中一个元素的大小是 20 b.

Table 2 Function Comparison Among the Proposed Scheme and the Related Schemes

表 2 本文方案与相关方案的功能对比

功能	本文方案	文献[8]	文献[9]	文献[33]	文献[34]	文献[35]	文献[41]	文献[23]	文献[25]	文献[26]
匿名性	√	√	√	×	×	×	√	√	√	√
抗假冒攻击	√	√	√	√	√	√	√	√	×	×
抗篡改攻击	√	√	√	√	√	√	√	×	×	×
抗重放攻击	√	×	×	×	×	×	√	√	√	√
机密性	√	√	√	×	×	×	×	×	×	×
可追溯性	√	√	√	√	√	√	√	√	×	×
抗 MHT	√	√	×	×	×	×	×	×	×	×

注:“√”表示实现了该功能;“×”表示不支持该功能.

① 在普通消息数量以及大量消息数量条件下本文方案的性能.为了评估发送方的计算开销,我们评估了密文生成需要的计算时间.在实验中,消息块分别从 0 增加到 100 和 1 000 个.如图 4 所示,在一般消息数量下,密文生成的时间成本随消息块的数量线性增加.具体而言,密文生成的时间为 0.162～1.613 s.如图 5 所示,在大量消息数量下,密文生成时间为 0.162～15.288 s.显然,这对发送者来说是完全可以接受的.

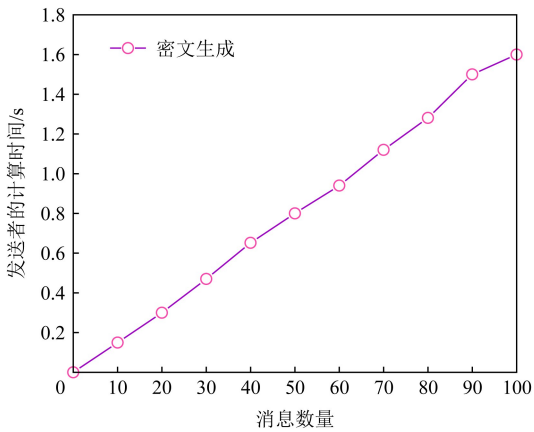

Fig. 4 Computation overhead of the sender

图 4 发送者的计算开销

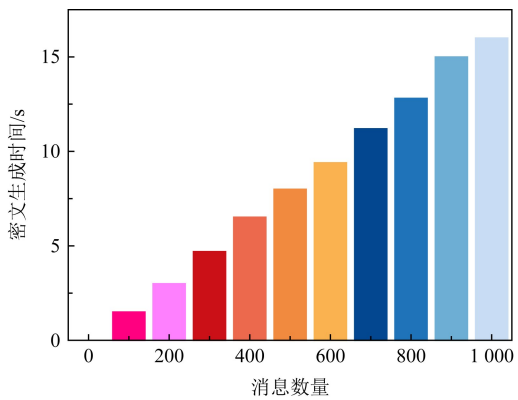

Fig. 5 Computation overhead of the sender

图 5 发送者的计算开销(大量消息)

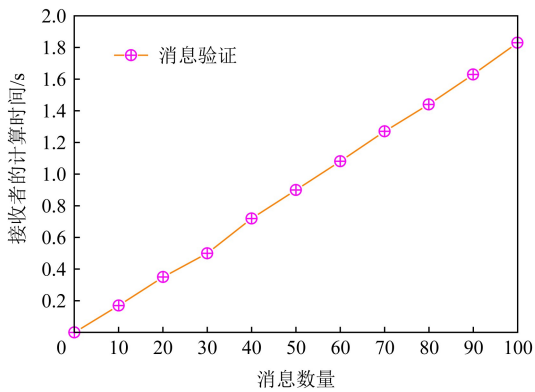

Fig. 6 Computation overhead of the receiver

图 6 接收者的计算开销

对于接收到的不同数量的消息,我们分别给出了在普通消息数量(0～100)以及大量消息数量(0～1 000)下的接收方的计算开销.如图 6 所示,接收者消息验证的计算开销随着发送消息的数量线性增加.接收者的计算开销从 0.18～1.825 s 不等.如图 7 所示,在消息数量为 0～1 000 时,接收方的计算开销从 0.18 s 增加到 17.98 s.

② 在普通消息数量条件下本文方案与文献[8-9,33-35]方案的性能比较.为了评估在一般消息数量的条件下,本文方案相较于文献[8-9,33-35]方案在性能方面是否有优势,我们分别将本文方案的发送方生成密文所需的计算时间以及接收方解密消息所需的计算时间与文献[8-9,33-35]方案进行了对比.如图 8 所示,文献[8]方案所需的密文生成计算时间最长.具体地,随着消息数量的增加,文献[8]方案的发送方所需的计算时间从 0 s 增加到 5.23 s.文献[9,33,35]方案的发送方的计算开销均大于本文方案.本文方案与实现相同功能的文献[8]方案相比

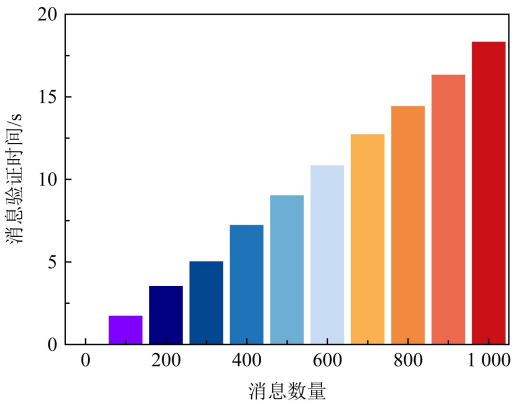

Fig. 7 Computation overhead of the receiver

图 7 接收者的计算开销(大量消息)

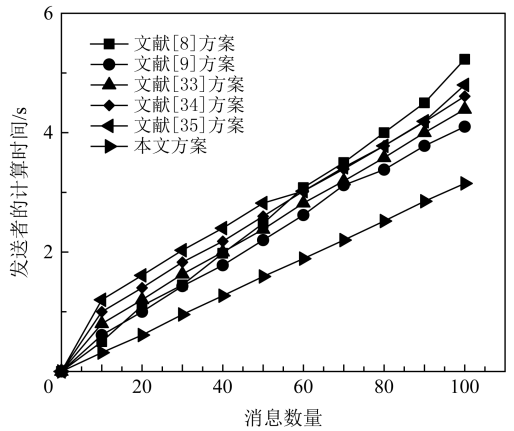

Fig. 8 Computation overhead of the sender

图 8 发送者的计算开销

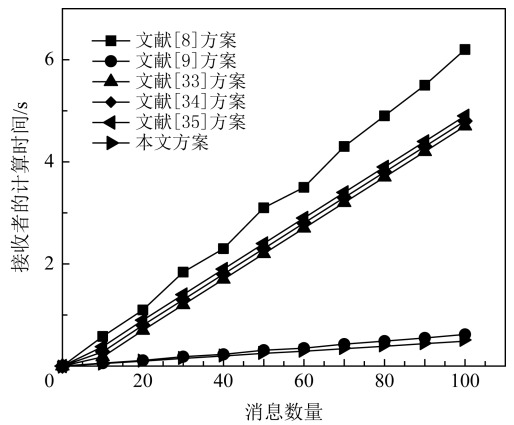

Fig. 9 Computation overhead of the receiver

图 9 接收者的计算开销

是非常高效的.同样地,如图 9 所示,文献[8]方案所需的密文解密计算时间最长,本文方案所需的密文解密计算时间最小.综上,本文方案与实现相同功能的方案相比是非常高效的.

7 总 结

本文提出了一个面向自动驾驶的高效可追踪的车联网匿名通信方案.在本文方案中,车辆由多辆车共享的属性集表示.由于属性集与车辆之间的 1 对多的关系,车辆的匿名性能自然地得到实现.此外,在本文方案中,指令消息以密文形式进行传输,也允许可信的权威(TA)通过传输的指令消息对恶意的车辆进行追溯和惩罚.此外,本文在属性基加密方案中融合了认证加密设计了一种签密方案作为底层技术支持本文提出的匿名通信方案.该签密方案相较于现存的属性基签密方案是高效的,更适用于自动驾驶场景.通过对其安全性的分析,该方案在安全性和效率上均达到了预期的效果.

作者贡献声明:侯慧莹负责算法与仿真实验的设计、实验数据的分析与处理、论文撰写;廉欢欢负责论文写作检查与修改;赵运磊负责算法设计、论文检查与修改.

参 考 文 献

[1] Chim T W, Yiu S M, Hui L C K, et al. SPECS: Secure and privacy enhancing communications schemes for VANETs [J]. Ad Hoc Network, 2011, 9(2): 189-203

[2] Zeadally S, Hunt R, Chen Y S, et al. Vehicular ad hoc networks (VANETs): Status, results, and challenges [J]. Telecommunication System, 2012, 50(4): 217-241

[3] Ghosh M, Varghese A, Gupta A, et al. Detecting misbehaviors in VANET with integrated root-cause analysis [J]. Ad Hoc Network, 2010, 8(7): 778-790

[4] Toor Y, Muhlethaler P, Laouiti A. Vehicle ad hoc networks: Applications and related technical issues [J]. IEEE Communications Surveys & Tutorials, 2008, 10(3): 74-87

[5] Zhang Yiming, She Kun, Hu Chenghua. Research on the classification method of safety cases in Internet of vehicles [J]. Journal of Information Security Research, 2020, 6(5): 433-440 (in Chinese)
(张一鸣, 佘堃, 胡成华. 车联网系统中的安全事件分级方法研究[J]. 信息安全研究, 2020, 6(5): 433-440)

[6] Wang Xiaoliang, Li Shuifan, Zhao Shujing, et al. A vehicular ad hoc network privacy protection scheme without a trusted third party [J]. Distribution Sensor Network, 2017, 13(12): 22-31

[7] Artail H, Abbani N. A pseudonym management system to achieve anonymity in vehicular ad hoc networks [J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 106-119

[8] Cui Hui, Deng R, Wang Guilin. An attribute-based framework for secure communications in vehicular ad hoc networks [J]. IEEE/ACM Transactions on Networking, 2019, 27(2): 721-733

[9] Kang Qian, Liu Xuejiao, Yao Yiyang. Efficient authentication and access control of message dissemination over vehicular ad hoc network [J]. Neurocomputing, 2016, 181: 132-138

[10] The Central People's Government of the People's Republic of China. Guide to the construction of national standard system of new generation artificial intelligence [OL]. [2020-10-19]. http://www.gov.cn/zhengce/zhengceku/2020-08/09content_5533454.htm (in Chinese)
(中华人民共和国中央人民政府. 国家新一代人工智能标准体系建设指南[OL]. [2020-10-19]. http://www.gov.cn/zhengce/zhengceku/2020-08/09 content _ 5533454. htm)

[11] Papadimitratos P, Kung A, Hubaux J, et al. Privacy and identity management for vehicular communication systems: A position paper [C/OL] //Proc of Workshop on Standards for Privacy in User-Centric Identity Management, 2006 [2020-10-19]. https://www.researchgate.net/publication/37439370_Privacy_and_Identity_Management_for_Vehicular_Communication_Systems_A_Position_Paper

[12] Golle P, Partridge K. On the anonymity of home/work location pairs [C] //Proc of the 7th Int Conf on Pervasive Computing. Berlin: Springer, 2009: 390-397

[13] Wiedersheim B, Ma Zhendong, Kargl F. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough [C] //Proc of the 7th Int Conf on Wireless On-demand Network Systems and Services. Piscataway, NJ: IEEE, 2010: 176-183

[14] Raya M, Hubaux J P. Securing vehicular ad hoc networks [J]. Computing Security, 2007, 15(1): 39-68

[15] Lu Rongxing, Lin Xiaodong, Zhu Haojin, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications [C] //Proc of IEEE INFOCOM. Piscataway, NJ: IEEE, 2008: 1229-1237

[16] Freudiger J, Raya M, Felegyhazi M, et al. Mix-zones for location privacy in vehicular networks [C/OL] //Proc of Workshop Wireless Network Intelligence Transportations. Piscataway, NJ: IEEE, 2007 [2020-10-19]. https://www.researchgate.net/publication/37450059_Mix-Zones_for_Location_Privacy_in_Vehicular_Networks

[17] Zhang Chenxi, Lin Xiaodong, Lu Rongxing, et al. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks [C] //Proc of IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2008: 1451-1457

[18] Zhang Chenxi, Lu Rongxing, Lin Xiaodong, et al. An efficient identity-based batch verification scheme for vehicular sensor networks [C] //Proc of IEEE INFOCOM 2008. Piscataway, NJ: IEEE, 2008: 816-824

[19] Zhang Chenxi, Ho P, Tapolcai J. On batch verification with group testing for vehicular communications [J]. Wireless Network, 2011, 17(8): 1851-1865

[20] Shamir A. Identity-based cryptosystems and signature schemes [C] //Proc of CRYPTO 1984. Berlin: Springer, 1984: 47-53

[21] Lee C, Lai Yanming. Toward a secure batch verification with group testing for VANET [J]. Wireless Network, 2013, 19(6): 1441-1449

[22] Horng S J, Tzeng S F, Pan Yi, et al. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET [J]. IEEE Transactions on Information Forensics Security, 2013, 8(11): 1860-1875

[23] 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

[24] Liu J K, Yuen T H, Au M H, et al. Improvements on an authentication scheme for vehicular sensor networks [J]. Expert System Application, 2014, 41(5): 2559-2564

[25] Zhang Jianhong, Xu Min, Liu Liying. On the security of a secure batch verification with group testing for VANET [J]. Network Security, 2014, 16(5): 355-362

[26] Bayat M, Barmshoory M, Rahimi M, et al. A secure authentication scheme for VANETs with batch verification [J]. Wireless Network, 2015, 21(5): 1733-1743

[27] Levente B, Tamas H, Istvan V. On the effectiveness of changing pseudonyms to provide location privacy in VANETs [C] //Proc of the 4th European Conf on Security and Privacy in Ad-hoc and Sensor Networks. Berlin: Springer, 2007: 129-141

[28] Beresford A, Stajano F. Mix Zones: User privacy in location-aware services [C] //Proc of the 2nd Annual Conf on Pervasive Computing and Communications Workshops. Piscataway, NJ: IEEE, 2004: 127-131

[29] Huang L, Matsuura K, Yamane H. Enhancing wireless location privacy using silent period [C] //Proc of 2005 IEEE Wireless Communications and Networking Conf (WCNC). Piscataway, NJ: IEEE, 2005: 1187-1192

[30] Kamat P, Baliga A, Trappe W. An identity-based security framework for VANETs [C] //Proc of the 3rd Int Workshop/Vehicular Ad Hoc Networks (VANET). Piscataway, NJ: IEEE, 2006: 94-95

[31] Calandriello G, Papadimitratos P, Hubaux J, et al. Efficient and robust pseudonymous authentication in VANET [C] //Proc of the 4th ACM Int Workshop on Vehicular Ad Hoc Networks. Piscataway, NJ: IEEE, 2007: 19-28

[32] Lin Xiaodong, Sun Xiaoting, Ho P. GSIS: A secure and privacy-preserving protocol for vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442-3456

[33] Yang Xu, Yi Xun, Khalil I, et al. A lightweight authentication scheme for vehicular ad hoc networks based on MSR [J]. Vehicular Communications, 2019, (15): 16-27

[34] Kamil I A, Ogundoyin S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks [J]. Journal of Information Security and Applications, 2019, (14): 184-200

[35] Chen Zhiya, Zhou Kunlin, Liao Qin. Quantum identity authentication scheme of vehicular ad-hoc networks [J]. International Journal Theoretical Physics, 2019, 58: 40-57

[36] Wen Hong, Ho P, Gong Guang. A novel framework for message authentication in vehicular communication networks [C/OL] //Proc of IEEE Global Communications Conf. Piscataway, NJ: IEEE, 2009[2020-10-19]. https://ieeexplore.ieee.org/document/5425519

[37] Zhang Lei, Wu Qianhong, Solanas A, et al. A scalable robust authentication protocol for secure vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2010, 59 (4): 1606-1617

[38] Qin Bo, Wu Qianhong, Domingo-Ferrer J, et al. Preserving security and privacy in large-scale VANETs [C] //Proc of Int Conf on Information and Communications Security. Berlin: Springer, 2011: 121-135

[39] Foster D, Kargl F, Lohr H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET) [C] //Proc of IEEE Vehicular Networking Conf (VNC). Piscataway, NJ: IEEE, 2014: 25-32

[40] Rogaway P. Authenticated-encryption with associated-data [C] //Proc of the 9th ACM Conf on Computer and Communications Security. Piscataway, NJ: IEEE, 2002: 98-107

[41] He Debiao, Zeadally S, Xu Baowen et al. An efficient identity-based conditional privacy-preserving authentication solution for vehicular ad hoc networks [J]. IEEE Transactions on Information Forensics Security, 2015, 10(12): 2681-2691

[42] Stanford. Pairing-Based Cryptography (PBC) Library [OL]. [2020-10-20]. https://crypto.stanford.edu/pbc/howto.html

[43] 2000—2020 Free Software Foundation. The GNU Multiple Precision Arithmetic Library (GMP) [OL]. [2020-10-20]. http://gmplib.org

Hou Huiying, born in 1992. PhD. Her main research interests include applied cryptography and information security, in particular, vehicle ad-hoc network security and attribute-based cryptology. (18110240036@fudan.edu.cn)

侯慧莹,1992 年生.博士.主要研究方向为应用密码学和信息安全,特别是车联网安全和属性基密码.

Lian Huanhuan, born in 1993. PhD. Her main research interests include cryptography, information security and lattice cryptography. (19110240032@fudan.edu.cn)

廉欢欢,1993 年生.博士.主要研究方向为密码学、信息安全和格密码.

Zhao Yunlei, born in 1974. PhD, distinguished professor at Fudan University. His main research interests include post-quantum cryptography, cryptographic protocols, and theory of computing.

赵运磊,1974 年生.博士,复旦大学特聘教授.主要研究方向为后量子密码、密码协议和计算理论.