

基于属性签名的车联网匿名信任管理方案

肖敏¹, 毛发英¹, 黄永洪¹, 曹云飞^{2,3}

(1. 重庆邮电大学网络空间安全与信息法学院, 重庆 400065; 2. 中国电子科技集团公司第三十研究所, 四川 成都 610041;
3. 中国电子科技网络信息安全有限公司, 四川 成都 610041)

摘要: 信任管理机制可以用来解决车联网(VANET)中消息的真实性评估和通信实体之间的信任问题。现有的信任管理方案中缺乏有效的隐私保护机制, 即在绑定车辆身份与其信誉值的关联时会暴露车辆的隐私。利用基于属性的签名具有的匿名性, 提出一种VANET匿名信任管理方案。由可信权威维护车辆的信誉等级, 将车辆的信誉等级和当前时间作为车辆的属性身份集合, 实现匿名的车辆身份与其信誉等级绑定, 能够提供车辆的隐私保护; 属性签名私钥的及时更新能够抵抗虚假信誉攻击; 属性签名验证的同时实现匿名验证车辆的信誉等级; 利用假名隐藏车辆的真实身份, 实现只有可信权威能够从假名解析车辆的真实身份以更新其信誉等级, 并提供恶意车辆身份合法和安全的追踪。在通用群模型下, 证明基于属性的签名方案满足不可伪造性的安全性。安全分析进一步表明, 所提方案能够保护车辆的身份和位置隐私, 实现只有可信权威可以合法追踪恶意车辆, 还能够提供抵抗虚假信誉攻击, 保证通信的完整性和抵抗重放攻击。性能分析验证了所提方案与已有方案相比, 具有一定的计算和通信效率优势。

关键词: 车联网; 信任管理; 条件隐私保护; 基于属性的签名

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023019

Anonymous trust management scheme of VANET based on attribute signature

XIAO Min¹, MAO Faying¹, HUANG Yonghong¹, CAO Yunfei^{2,3}

1. School of Cyberspace Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. No.30 Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, China
3. China Electronics Technology Cyber Security Co., Ltd, Chengdu 610041, China

Abstract: Trust management mechanisms can solve the authenticity assessment problem of messages and establish trust between communication entities in the VANET. However, current trust management schemes lack an effective privacy protection mechanism, leading to privacy concerns for vehicles when binding their identity with their trust level. Based on the anonymity of attribute-based signature, an anonymous trust management scheme was proposed

收稿日期: 2022-06-12; 修回日期: 2023-03-02

通信作者: 肖敏, xiaomin@cqupt.edu.cn

基金项目: 四川省重点研发计划(2020YFG0292)

Foundation Item: The Key R&D Project of Sichuan Province (2020YFG0292)

引用格式: 肖敏, 毛发英, 黄永洪, 等. 基于属性签名的车联网匿名信任管理方案[J]. 网络与信息安全学报, 2023, 9(2): 33-45.

Citation Format: XIAO M, MAO F Y, HUANG Y H, et al. Anonymous trust management scheme of VANET based on attribute signature[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 33-45.

for VANET. The trust level of the vehicle was maintained by the trusted authority. The trust level of vehicles and the current time were taken as the attribute identity set of the vehicle, so as to realize the binding of the anonymous vehicle identity with its trust level, which could provide the privacy protection of vehicles. In addition, the timely update of attribute signature private key could resist false reputation attack and the trust level of the vehicle could be verified anonymously while the attribute signature was verified. Furthermore, the pseudonym was used to hide the real identity of the vehicle, enabling only the trusted authority could parse the real identity of vehicles from the pseudonym to update their trust level, and providing legal and secure tracking of the malicious vehicle identity vehicle. Under the general group model, the attribute-based signature scheme is proven to satisfy the security of unforgeability. The security analysis further shows that the scheme protects the identity and location privacy of vehicles, enables only the trusted authority to legally track malicious vehicles, resists false reputation attacks, ensures communication integrity, and resists replay attacks. Performance analysis confirms that the proposed scheme has better computation and communication efficiency than existing schemes.

Keywords: VANET, trust management, conditional privacy preserving, attribute-based signature

0 引言

车载网 (VANET, vehicular ad-hoc network) 是专门为车辆间通信而设计的自组织网络, 每个车辆都配置了无线通信设备和传感设备, 使得车辆与车辆、车辆与路侧单元 (RSU, road side unit) 能够进行通信^[1], 共享如交通事故、道路状况等交通安全信息, 及时获知交通环境, 进而改善交通安全性和效率。但是, 如果合法节点恶意广播虚假消息, 将扰乱网络的正常运行, 带来严重的交通安全隐患^[2]。因此, 如何有效识别恶意车辆以及虚假消息成为 VANET 中必须解决的重要问题。

信任管理机制^[2-5]作为 VANET 的安全措施, 是解决该问题的主要方法, 其根据车辆在 VANET 中的行为, 建立所有车辆的信誉体系, 帮助车辆识别诚实可信的交互方, 判断收到的消息是否真实可靠。同时, 利用奖惩机制进行信誉的实时更新, 激励节点积极合作并提供诚信的服务^[2]。

VANET 具有移动易变且通信信道开放的特点, 这让恶意车辆的识别和消息真实可靠性的验证面临许多挑战^[6]。构建 VANET 信任管理要求长期跟踪车辆的历史信誉信息, 但这与车辆的隐私保护存在冲突。所以, 信任管理过程需要实现匿名绑定车辆及其信誉值 (或等级) 并保证信誉的不断更新。另外, VANET 信任管理中的完全匿名可能会增加恶意车辆从事破坏活动并且逃避追责

的风险。例如, 车辆滥用匿名性可能会发起选择性行为攻击, 此攻击意味着一个诚实合法的车辆节点突变为恶意节点在网络中做出恶意为^[4]。例如, 发送大量同一事件报告消息造成信誉管理过程堵塞。因此, 隐私保护必须是有条件的, 在恶意事件发生时可以追踪恶意车辆的身份。

VANET 信任管理研究中已有一些隐私保护及其条件隐私保护机制, 如通过信誉管理中心颁发的信誉证书^[7]或假名^[7-13]实现信誉的证明及其身份隐私保护。文献[7]提出一种集中式的匿名信誉管理系统。发送车辆 A 将包含其信誉证书和假名证书的消息经多个中间车辆评估后转发至接收车辆 B, B 生成反馈消息发送至信誉服务器更新 A 的信誉。转发过程中多个中间车辆将信誉证书和假名证书附加到消息中, 隐藏发送者证书信息, 但证书的多次应用仍然会暴露车辆的位置隐私。文献[8]提出了一种基于身份签名和假名的信任管理方案。车辆与 RSU 之间的通信都使用主假名但未进行更换, RSU 可以轻松关联同一主假名的车辆行为, 从而暴露了车辆的位置隐私。文献[9]提出了一种由车辆自我管理的信誉模型。方案中每个车辆改变假名时都要同时宣布其以前和新的假名, 使得其他车辆可以链接两个假名相关的消息, 暴露车辆的位置隐私。

基于信誉证书或假名证书的方法运用于 VANET 信任管理存在一些挑战: 为了维护车辆的信誉数据, 需要持续追踪车辆在网络中的行为活动, 但这与车辆隐私保护相矛盾。利用假名隐藏

车辆真实身份,需要设计有效的假名变更机制实现位置隐私^[10]。如果仍然采用信誉证书证明车辆的信誉,为了实现身份隐私,只能直接将假名与信誉证书绑定,频繁的假名变更会使得信誉证书的管理非常复杂,最终导致信誉维护和更新不能实现。因此,需要另外一种机制在车辆共享信息过程中提供对信誉的证明和实现持续的信誉更新,其不能关联车辆的任何身份信息,包括掩盖真实身份的假名。文献[11-13]的方案同样提出使用假名保护信任管理过程中车辆的身份隐私,但未提出有效的假名更改策略,存在隐私泄露的风险,且方案中没有考虑可追溯性,无法实现对恶意车辆真实身份进行追责惩罚。

还有一些研究工作使用环签名^[14]或群签名^[15-16]等方法可以实现较好的匿名性,保护车辆的隐私。Liu等^[14]提出了VANET中基于区块链的信任管理模型,设计了一种具有条件隐私保护的广告方案。但是该方案未解决在保障条件隐私保护的前提下提供车辆信誉的证明;并且,方案中使用区块链地址作为假名,若长期使用一个地址会存在暴露车辆位置隐私的风险;另外,该方案采用环签名方法,其造成的计算开销和通信开销与环签名中身份环长的大小呈现线性增长的关系。Chen等^[15]提出了VANET中基于群签名的具有隐私保护的信任管理方案。群签名认证隐藏了发送者的身份,模糊了身份与签名的关联性。但该方案签名以及验证计算开销比较大,会造成较高的时延,降低消息认证的效率;并且所有车辆的信誉数据都由信誉服务器收集并进行计算更新,管理中心的维护成本较大,实用性不好。

针对VANET中信任管理存在的以上问题,本文提出了一种基于属性签名和假名相结合的具有条件隐私保护的匿名信任管理方案。基于属性的签名作为数字签名的延伸,只有当用户的属性集合满足访问结构时才能生成有效的签名^[17]。签名验证成功,则表明签名用户具有满足访问结构的属性值,但不会暴露车辆的真实身份。本文主要的工作内容如下。

1) 为车辆颁发属性签名私钥实现匿名的车辆实体与其信誉等级的绑定,将信誉等级属性和时间属性作为签名属性,通过签名验证实现车辆

信誉等级的匿名验证,并且时间属性可以控制车辆信誉等级的匿名更新。

2) 设计合适的假名结构实现与车辆真实身份的隐秘关联,使得只有可信权威能够追踪恶意车辆,防止合法授权的车辆滥用匿名性产生恶意行为。

3) 利用属性签名方案,对发送的信誉管理相关的消息(如事件报告消息)进行签名,提供消息源的认证和消息完整性保护。

1 系统模型与安全目标

1.1 系统模型

本文方案的系统模型如图1所示,主要包括的实体为可信权威(TA, trusted authority)、RSU和车辆。

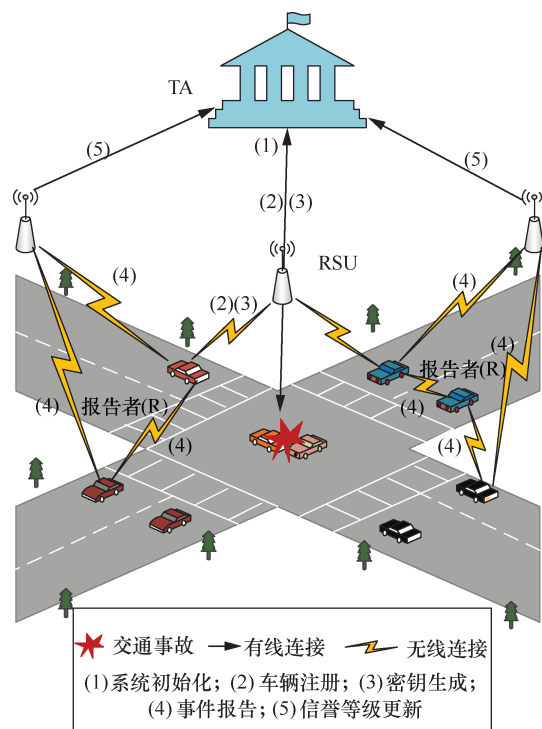


图1 系统模型

Figure 1 System model

TA主要负责车辆的注册和信誉信息维护,并且为系统中的合法车辆颁发属性密钥,另外,可以根据发送的消息追踪车辆的真实身份;RSU收集车辆发送的报告消息(RM, report message)。通过RM中获取的车辆信誉等级计算车辆的信誉更新值,之后将信誉更新值反馈给TA以更新车辆的信誉等级。本文方案中假定发送预警事件

的车辆作为报告者 (R, reporter), 其在系统中主动报告交通状况的车辆, 并通过签名生成 RM 发送给邻近的车辆和 RSU 来提升自身的信誉等级。

1.2 安全目标

假设 RSU 为半可信实体, 易遭受外部攻击, 车辆是不可信的, 可能存在恶意车辆对信任管理过程实施攻击。本文方案主要实现的安全目标如下。

1) 身份隐私: 为实现车辆身份隐私保护, 只有 TA 可以获得车辆的真实身份, 其余实体均不能通过车辆发送的消息和假名获得发送者的真实身份。

2) 位置隐私: 确保攻击者无法链接同一车辆多次参与信誉管理时发送的消息以及使用的假名, 保护车辆的位置隐私。

3) 追踪恶意车辆: 在发现恶意车辆的情况下, 有且只有 TA 能够追踪到车辆的真实身份, 以对其进行处罚。

4) 抵抗虚假信誉攻击: 防止恶意车辆对信誉等级造假或者应用过期的信誉等级破坏信誉管理过程。

5) 通信安全性: 保证通信数据的完整性和数据源真实性及其抵抗重放攻击。

2 方案设计

本文方案将信誉等级和时间作为属性, 利用基于属性的签名机制实现具有隐私保护特性的车辆信誉管理, 并保障信誉管理过程的安全。本文方案包括 5 个阶段: 系统初始化、车辆注册、密钥生成、事件报告和信誉等级更新。

2.1 系统初始化

假设系统中所有实体都拥有一对长期的公私钥对, 选用任意的安全密码机制, 保护实体之间通信的安全性。

(1) 系统属性和访问结构设置

根据信誉更新的频率要求, 将一段较长的时期 (如一年) 划分为等长的时隙 (如一天)。设时隙集合为 $TS = \{L_1, L_2, \dots, L_l\}$, 该集合即系统的时间属性集合。时隙集合随着时间的推移不断更新, 因此系统的时间属性永不重复。另外, 将车辆的信誉划分为 l 个信誉等级 $TrustL$ 的集合 $TL = \{L_1, L_2, \dots, L_l\}$, 该集合即系统的信誉等级属性集合。

(2) 基于属性的签名方案

文献[18]建议的基于属性的签名 (ABS, attribute based signature) 方案, 包括 4 个算法: 初始化 $Setup(\lambda) \rightarrow (PP, MK)$ 、属性密钥生成算法 $KeyGen(MK, Q) \rightarrow (SK)$ 、签名算法 $Sign(PP, SK, m, \Gamma) \rightarrow (\sigma)$ 以及验证算法 $Verify(PP, \sigma, m, \Gamma) \rightarrow (accept/reject)$ 。

算法 1 $Setup(\lambda) \rightarrow (PP, MK)$

该算法由 TA 执行, 根据系统安全参数 λ , 输出系统的公共参数 PP 和系统主密钥 MK。TA 根据安全参数 λ 选择 3 个素数 q 阶循环群 G_1, G_2, G_T , 定义双线性映射 $e: G_1 \times G_2 \rightarrow G_T$, 随机选取 $a_0, a, b, c, d \in Z_p^*$, 以及生成元 $g \in G_1$ 和 $h_0, h_1, h_2 \in G_2$, 并计算 $C = g^c$, $PK_{TA} = g^d$, $E_0 = h_0^{a_0}$, $E_j = h_j^a$, $F_j = h_j^b$, $\forall j \in \{1, 2\}$, 定义两个哈希函数 $H: \{0, 1\}^* \rightarrow Z_p^*$ 和 $H_1: G_1 \rightarrow Z_p$ 。TA 安全保存主密钥 $MK = (a_0, a, b, c, d)$, 其中 d 为 TA 的私钥 SK_{TA} , 将公共参数 $PP = (H, H_1, C, PK_{TA}, g, h_0, h_1, h_2, E_0, E_1, E_2, F_1, F_2)$ 公布到系统中。设时间属性和信誉等级属性都取值于 Z_p^* , 表示为 $TS = \{T_i \in Z_p^*, i=1, 2, \dots, s\}$, $TL = \{L_j \in Z_p^*, j=1, 2, \dots, l\}$ 。

算法 2 $KeyGen(MK, Q) \rightarrow (SK)$

算法 2 由 TA 执行, 该算法为属性集为 Q 的车辆生成属性签名私钥 SK。在时隙 T_i , 具有信誉等级 L_j 的车辆的属性集为 $Q = \{T_i, L_j\}$ 。TA 随机选择一个生成元 $K_{base} \in G_1$, 然后计算 $K_0 = (K_{base})^{1/a_0}$, $K_{T_i} = (K_{base})^{1/(a+bT_i)}$, $K_{L_j} = (K_{base})^{1/(a+bL_j)}$, 得到属性签名私钥 $SK = (K_{base}, K_0, K_{T_i}, K_{L_j})$ 。在当前的时隙 T_c , 具有信誉等级 $L(V) \in TL$ 的车辆 V 的属性签名私钥记为 $SK_V = (K_{V, base}, K_{V, 0}, K_{V, T_c}, K_{L(V)})$ 。

算法 3 $Sign(PP, SK, m, \Gamma) \rightarrow (\sigma)$

该算法由发送消息的车辆执行, 利用签名私钥 SK 和访问结构 $\Gamma = \Gamma_{ij} = T_i \wedge L_j$ 对发送的消息 $m \in \{0, 1\}^*$ 进行签名, 输出签名 σ 。根据文献[18]中的方法可以将访问结构 $\Gamma_{ij} = T_i \wedge L_j$ 转换为对应的访问矩阵 $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 车辆计算签名如下。

① 求解向量 $\mathbf{v} = (v_1, v_2)$ ，使得 $\mathbf{vM} = [1, 0]$ ，显然， $\mathbf{v} = (v_1, v_2) = (1, -1)$ 。

② 计算 $\mu = H(m)$ 。

③ 随机选取 $r_0 \in Z_p^*$ 和 $r_1, r_2 \in Z_p$ ，计算

$$Y = (K_{\text{base}})^{r_0}, \quad W = (K_0)^{r_0} \quad (1)$$

$$S_1 = (K_{T_i}^{v_1})^{r_0} \cdot (Cg^\mu)^{r_1} = (K_{T_i})^{r_0} \cdot (Cg^\mu)^{r_1} \quad (2)$$

$$S_2 = (K_{L_j}^{v_2})^{r_0} \cdot (Cg^\mu)^{r_2} = (K_{L_j})^{-r_0} \cdot (Cg^\mu)^{r_2} \quad (3)$$

$$P_1 = (E_1 F_1^{T_i})^{M_{11} r_1} \cdot (E_1 F_1^{L_j})^{M_{21} r_2} = (E_1 F_1^{T_i})^{r_1} \quad (4)$$

$$P_2 = (E_2 F_2^{T_i})^{M_{12} r_1} \cdot (E_2 F_2^{L_j})^{M_{22} r_2} = (E_2 F_2^{T_i})^{r_1} \cdot (E_2 F_2^{L_j})^{r_2} \quad (5)$$

签名结果 $\sigma = (m, \Gamma_{ij}, Y, W, S_1, S_2, P_1, P_2)$ 。车辆 V 在访问结构 Γ_V 下对消息 m 的签名记为 $\sigma_V^{\Gamma_V}(m)$ 。

算法 4 $\text{Verify}(\text{PP}, \sigma, m, \Gamma) \rightarrow (\text{accept/reject})$

该算法由接收消息的实体执行。根据系统公共参数，验证对消息 m 的签名 $\sigma = (m, \Gamma_{ij}, Y, W, S_1, S_2, P_1, P_2)$ 是否正确，输出接受 (accept) 或拒绝 (reject)。根据访问结构对应的访问矩阵 $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 和 $\mu = H(m)$ ，检查以下式子是否成立。

$$e(W, E_0) = e(Y, h_0) \quad (6)$$

$$e(S_1, (E_1 F_1^{T_i})^{M_{11}}) \cdot e(S_2, (E_1 F_1^{L_j})^{M_{21}}) = e(Y, h_1) e(Cg^\mu, P_1) \quad (7)$$

$$e(S_1, (E_2 F_2^{T_i})^{M_{12}}) \cdot e(S_2, (E_2 F_2^{L_j})^{M_{22}}) = e(Cg^\mu, P_2) \quad (8)$$

若式(6)、式(7)、式(8)都成立，则输出 accept，否则输出 reject。

本文所用方案是文献[18]方案在实践中的具体应用，与原方案的不同之处在于本文 ABS 中的访问结构只包括时间属性 T_i 和信誉等级属性 L_j 的与运算结构 $\Gamma_{ij} = T_i \wedge L_j$ ，因此该方案不能实现签名用户的属性隐私，而且信誉管理过程需要利用公开的车辆信誉等级属性。本文方案利用 ABS 的匿名性和假名机制实现信誉管理过程的身份和位置隐私。ABS 的匿名性体现在 ABS 中只包含

通用的时间和信誉等级属性，没有包含任何与车辆身份相关的信息。下面给出 ABS 不可伪造性的定义。

定义 1^[18] 如果任意多项式时间的敌手 $\mathcal{A}$ 在和挑战者 $\mathcal{C}$ 的游戏中成功的优势是可忽略的，则称基于属性的签名算法具有不可伪造性。

初始化阶段。挑战者 $\mathcal{C}$ 输入安全参数 λ ，运行 $\text{Setup}(\lambda)$ 算法得到系统的公共参数 PP，并将 PP 发送给敌手 $\mathcal{A}$ 。

询问阶段。敌手 $\mathcal{A}$ 可以发起如下询问。

① 密钥生成询问。敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 发出属性集合 Q_i 的密钥生成请求， $\mathcal{C}$ 返回相应属性签名私钥 SK_{Q_i} 。

② 签名询问。敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 发送 (m_j, Γ_j) 请求签名，挑战者 $\mathcal{C}$ 返回对应的签名 $(m_j, \Gamma_j, \sigma_j)$ 。

敌手 $\mathcal{A}$ 输出签名 $(m^*, \Gamma^*, \sigma^*)$ 。

如果敌手 $\mathcal{A}$ 没有询问过满足访问结构 Γ^* 的任何属性集的私钥，也没有询问过 (m^*, Γ^*) 的签名，且 $\text{Verify}(\text{PP}, m^*, \Gamma^*, \sigma^*) = \text{accept}$ ，则称敌手 $\mathcal{A}$ 在该游戏中获得成功。

2.2 车辆注册

当新车辆 V 加入系统中时，向 TA 提供自己的真实身份信息进行验证，若验证通过，TA 为车辆分配唯一身份标识 $\text{RID}_V \in Z_p$ ，并初始化车辆的信誉等级为 L_0 。

之后，TA 将注册成功车辆的信息记入其维护的车辆信息表（如表 1 所示）中。其中，属性密钥参数 $K_{\text{base}} \in G_1$ 是车辆请求属性私钥时产生的用于生成属性私钥的公共基底，初始值为空 (Null)； $T_{\text{base}} \in Z_p^*$ 为生成属性私钥时对应的时隙，初始值为车辆注册时对应的时隙，在车辆请求属性私钥时进行更新。在时隙 T_s 注册到系统的车辆 V 的信息记录为 $(\text{RID}_V, L_0, (\text{Null}, T_s))$ 。

表 1 车辆信息

Table 1 Vehicle information	
符号	信息
RID	身份标识
TrustL	信誉等级
$(K_{\text{base}}, T_{\text{base}})$	属性密钥参数

2.3 密钥生成

想要参与信誉管理的车辆首先需要向 TA 申请当前时隙的属性签名私钥并生成假名 (PID, pseudonym identity), 用于对发送消息进行签名, 证明自己的信誉等级并保护自己的隐私。

(1) 车辆属性签名私钥生成

车辆 V 由安全信道向 TA 发送属性私钥请求 REQ_{SK}, 请求中包括车辆的真实身份标识 RID _{V} 和时间戳等信息。TA 根据 REQ_{SK} 中的真实身份标识 RID _{V} 查找车辆信息表中该车辆的信誉等级为 TrustL = $L(V) \in TL$ 。

为了激励车辆积极参与信誉管理, TA 可以通过如下方式进行信誉等级的更新。

① 计算 $\Delta T = T_c - T_{base}$, T_c 为系统当前时隙, T_{base} 是信息表中记录的上一次密钥请求 (即信誉更新) 的时隙, ΔT 即该车辆两次参与信誉管理的时间间隔。

② 如果 ΔT 过大, 超过某个阈值 T_0 (由系统初始化时设置), TA 根据事先制定的规则, 如文献[19]方案中给出的 $L(V)^* = L(V) \cdot \alpha^{\Delta T}$ (其中 $\alpha \in (0,1)$ 表示为时间衰落因子, 是由系统设置的参数), 以实施惩罚, 更新信誉等级为 $L(V)^*$, 从而车辆的属性集更新为 $Q^* = \{L(V)^*, T_c\}$ 。

针对更新的属性集, TA 运行属性签名的 KeyGen(MK, Q^*) 算法, 得到车辆 V 的属性签名私钥, 记为 $SK_V = (K_{V,base}, K_{V,0}, K_{V,T_c}, K_{L(V)^*})$; TA 用最新的 (K_{base}, T_c) 更新车辆 V 信息表中对应的属性密钥参数 (K_{base}, T_{base}) 。

(2) 假名生成

在执行私钥生成算法的同时, TA 利用自己的公钥和车辆 V 的真实身份产生车辆的假名, 该假名和属性私钥一起用于一次信任管理过程。具体方法如下。随机选择 $k_V \in Z_p^*$ 并计算

$$D_{V,1} = g^{k_V} \quad (9)$$

$$D_{V,2} = RID_V \oplus H_1(PK_{TA}^{k_V}) \quad (10)$$

得到车辆的假名 $PID_V = (D_{V,1}, D_{V,2}, \text{Sign}_{SK_{TA}}(D_{V,1} \parallel D_{V,2}))$, 其中 $\text{Sign}_{SK_{TA}}(D_{V,1} \parallel D_{V,2})$ 是 TA 对假名的签名, 用于防止车辆自己生成不符合规则的假名逃避追踪。

属性私钥 SK_V 和对应的假名 PID_V 被 TA 安全

发送给车辆 V 。

2.4 事件报告

在当前时隙 T_c , 设事件报告者为车辆 R , 具有信誉等级 $L(R)^*$, 其主动向周围车辆报告事件消息 $m \in \{0,1\}^*$ 。为了证明事件消息 m 的来源和报告者的信誉等级并保证消息不被篡改, 车辆 R 运行基于属性的签名算法 $\text{Sign}(PP, SK_R, m \parallel TS_R \parallel PID_R, \Gamma_R)$ 对报告内容 $(m \parallel TS_R \parallel PID_R)$ 进行签名, 其中 PP 是系统公共参数, $SK_R = (K_{R,base}, K_{R,0}, K_{R,T_c}, K_{L(R)^*})$ 是车辆 R 的属性签名私钥, PID_R 为车辆 R 的假名, TS_R 表示事件报告的时间戳, 访问结构 $\Gamma_R = T_c \wedge L(R)^*$, 得到签名结果为 $\sigma_R^{\Gamma_R}(m \parallel TS_R \parallel PID_R)$, 车辆 R 将关于事件 m 的报告消息 $RM_R = \{m, TS_R, PID_R, \sigma_R^{\Gamma_R}(m \parallel TS_R \parallel PID_R), \Gamma_R\}$ 发送给附近的车辆以及 RSU 进行信誉计算。

2.5 信誉等级更新

接收车辆或 RSU 接收到报告消息 RM_R , 首先检查时间戳 TS_R 是否有效, 有效则运行签名验证算法 $\text{Verify}(PP, \sigma_R^{\Gamma_R}(m \parallel TS_R \parallel PID_R), (m, TS_R, PID_R), \Gamma_R)$ 验证签名的正确性。如果签名有效, 接收车辆或 RSU 由报告消息可以获得报告车辆 R 的信誉等级 $L(R)^*$ 。接收车辆和 RSU 还可以根据事件内容的真实性判断报告者 R 是否存在恶意行为, 并且向 TA 进行举报, 可由 TA 对恶意车辆进行惩罚 (对于恶意行为举报过程, 本文不再重点详述)。

对车辆信誉产生影响的因素除了车辆诚实或恶意的行为, 还有车辆报告不同级别的事件以及车辆报告的顺序等。参考文献[20]中更新信誉的方法, 将车辆 R 报告的预警事件分为 3 个级别 ($L=1,2,3$): 一是当车辆 R 失去控制时, 会自动广播一级警报信息, 避免发生碰撞; 二是当车辆 R 在改变其驾驶状态之前 (如紧急变道或制动) 广播二级预警消息; 三是当出现交通事故或道路损坏引发道路阻塞时广播三级警报消息。另外, 为激励车辆积极主动报告事件消息, 可以将 $S=0,1,\dots,n$ 表示为报告者 R 发送报告消息的顺序, 并根据如式(11)所示的奖惩规则计算每个报告者 R 的信誉更新值 Cr 。

$$\begin{aligned} \text{Re} &= \alpha \cdot \frac{1}{e^s \cdot L} \\ \text{Pu} &= (-1) \cdot \beta \cdot \frac{1}{e^s \cdot L} \\ \text{Cr} &= \text{Re or Pu} \end{aligned} \quad (11)$$

其中, α 和 β 分别表示奖励因子和惩罚因子 (由系统初始化时设定)。车辆诚实且积极主动地报告事件消息将获得信誉等级的提升奖励; 相反, 若车辆恶意或消极地报告事件消息, 其信誉等级会相应被降低。RSU 将参与信任管理的每一个车辆 V 的信用数据 ($\text{TS}_{\text{RSU}}, \text{Cr}, \text{PID}_V$) 发送给 TA 进行信誉等级的更新。

TA 接收到信用数据后, 首先利用车辆 V 的假名 $\text{PID}_V = (D_{V,1} = g^{k_V}, D_{V,2} = \text{RID}_V \oplus H_1(\text{PK}_{\text{TA}}^{k_V}))$ 和 TA 的私钥 d 解析出车辆的身份标识, 具体计算方法为 $\text{RID}_V = D_{V,2} \oplus H_1(D_{V,1}^d) = D_{V,2} \oplus H_1(g^{k_V \cdot d}) = D_{V,2} \oplus H_1(\text{PK}_{\text{TA}}^{k_V})$ 。

TA 利用解析出的 RID_V 检索车辆信息表, 获得车辆 V 的信誉等级 $L(V)^*$, 然后利用式(12)所示的方法更新车辆的信誉等级, 其中, l 表示划分的信誉等级的个数。

$$\begin{aligned} \text{TrustL}(V) &= L(V)^* + (l - L(V)^*) \cdot \text{Cr}, \text{Cr} = \text{Re} \\ \text{TrustL}(V) &= L(V)^* \cdot (1 + \text{Cr}), \text{Cr} = \text{Pu} \end{aligned} \quad (12)$$

显然, 车辆真实身份解析过程可以直接用于恶意车辆的真实身份追踪。

3 安全性证明与分析

在 ABS 方案的安全性证明的基础上进行本文方案的安全性分析。

3.1 安全性证明

定理 1 在通用群模型下, 2.1 节所述的 ABS 方案具有不可伪造性。

证明 通用群模型下, 敌手 $\mathcal{A}$ 只能对群元素进行规范的群操作和双线性操作, 即给定一个具有生成元 g 的循环群 G 的元素 $g^{x_1}, g^{x_2}, \dots, g^{x_n}$, 敌手 $\mathcal{A}$ 只能得到形式为 $g^{f(x_1, x_2, \dots, x_n)}$ 的输出, 其中, f 是一个多元线性多项式函数。本文所述签名方案的密钥和签名都只在群 G_1 和 G_2 上, 没有双线性运算, 所以通用群模型的敌手 $\mathcal{A}$ 在伪造签名时不能应用双线性操作。下面, 应用通用群模型的敌手

$\mathcal{A}$ 在定义 1 的游戏中获胜的群元素来分析本文所用 ABS 方案的不可伪造性。

考虑在 ABS 中定义的两个循环群 G_1 和 G_2 , 如果 $G_1 = G_2$, 则来自两个群的元素可以混合进行群运算, 通用群模型的敌手 $\mathcal{A}$ 能得到更多的运算结果, 对敌手 $\mathcal{A}$ 更为有利, 因此, 在下面的证明中假设 $G_1 = G_2$ 。

在此假设基础上, 设定这两个群的共同生成元 g , 在定义 1 的游戏中敌手 $\mathcal{A}$ 能够得到的所有群元素用生成元 g 表示如下。

① 初始化阶段。敌手 $\mathcal{A}$ 获得系统公共参数 $\text{PP} = \{g, C = g^c, \text{PK}_{\text{TA}} = g^d, h_0 = g^{\Delta_0}, E_0 = g^{e_0}, h_j = g^{\Delta_j}, E_j = g^{\Delta_j^a}, F_j = g^{\Delta_j^b} (j=1, 2)\}$ 。

② 密钥询问。敌手 $\mathcal{A}$ 第 k 次询问属性集 $Q^{(k)} = (T^{(k)}, L^{(k)})$ 的密钥, 得到

$$\text{SK}_{Q^{(k)}} = \left\{ \begin{aligned} K_{\text{base}}^{(k)} &= g^{x^{(k)}}, K_{T^{(k)}}^{(k)} = g^{x^{(k)} / (a + bT^{(k)})} \\ K_0^{(k)} &= g^{x^{(k)} / a_0}, K_{L^{(k)}}^{(k)} = g^{x^{(k)} / (a + bL^{(k)})} \end{aligned} \right\} \quad (13)$$

其中, $x^{(k)} \in Z_p^*$ 为随机数。假设总共询问 I 次, 即 $k \in \{1, 2, \dots, I\}$ 。

③ 签名询问。敌手 $\mathcal{A}$ 第 q 次询问 $(m^{(q)}, \Gamma^{(q)} = T^{(q)} \wedge L^{(q)})$ 的签名, 得到挑战者 $\mathcal{C}$ 返回的签名。观察签名中各项 $(Y, W, S_1, S_2, P_1, P_2)$ 的结构, Y, S_1, S_2 这 3 项的离散对数用随机数完全随机化, 剩余 3 项 W, P_1, P_2 中没有出现新的随机数, 即 Y, S_1, S_2 确定, 意味着 W, P_1, P_2 随之确定。因此, 从敌手 $\mathcal{A}$ 的视角, 签名可以表达为更为简洁的形式 $\sigma^{(q)} = (g^{y^{(q)}}, g^{y^{(q)} / a_0}, g^{s_1^{(q)}}, g^{s_2^{(q)}}, g^{p_1^{(q)}}, g^{p_2^{(q)}})$, 其中 $s_1^{(q)}, s_2^{(q)} \in Z_p, y^{(q)} \in Z_p^*$ 为随机数, $p_1^{(q)} = \frac{\Delta_1}{c + \mu^{(q)}} = [s_1^{(q)}(a + bT^{(q)}) - y^{(q)}], p_2^{(q)} = \frac{\Delta_2}{c + \mu^{(q)}} = [s_1^{(q)}(a + bT^{(q)}) + s_2^{(q)}(a + bL^{(q)})]$, 假设共询问了 J 次, 即 $q \in \{1, 2, \dots, J\}$ 。表 2 为敌手 $\mathcal{A}$ 在游戏中获取的以 g 为底的离散对数项。

敌手 $\mathcal{A}$ 利用表 2 中获得的所有项进行伪造签名。假设 $\mathcal{A}$ 输出消息 m^* 关于访问结构 $\Gamma^* = T^* \wedge L^*$ 的伪造签名 $\sigma^* = (g^{y^*}, g^{\omega^*}, g^{s_1^*}, g^{s_2^*}, g^{p_1^*}, g^{p_2^*})$, 满足 $y^* \neq 0, \omega^* \neq 0$ 及其对所有的 $q \in \{1, 2, \dots, J\}$ 有 $(m^*, \Gamma^*) \neq (m^{(q)}, \Gamma^{(q)})$ 和所有的

$k \in \{1, 2, \dots, I\}$ 有 $\Gamma^*(Q^{(k)}) \neq 1$ 。设 $\mu^* = H(m^*)$ ，如果该签名能够通过验证，则必须有

$$y^* = \omega^* a_0 \quad (14)$$

$$(c + \mu^*) p_1^* + \Delta_1 y^* = \Delta_1 s_1^* (a + bT^*) \quad (15)$$

$$(c + \mu^*) p_2^* = \Delta_2 [s_1^* (a + bT^*) + s_2^* (a + bL^*)] \quad (16)$$

表2 敌手在游戏中获取的以 g 为底的离散对数项
Table 2 The discrete logarithm base g acquired by the adversary in the game

算法阶段	离散对数项
初始化	$1, c, d, \Delta_0 a_0, \Delta_1, \Delta_2, \Delta_1 a, \Delta_2 a, \Delta_1 b, \Delta_2 b$
密钥询问	$x^{(k)}, x^{(k)} / a_0, x^{(k)} / (a + bT^{(k)}), x^{(k)} / (a + bL^{(k)}), k \in \{1, 2, \dots, I\}$
	$y^{(q)}, y^{(q)} / a_0, s_1^{(q)}, s_2^{(q)}$
签名询问	$p_1^{(q)} = \frac{\Delta_1}{c + \mu^{(q)}} [s_1^{(q)} (a + bT^{(q)}) - y^{(q)}],$ $p_2^{(q)} = \frac{\Delta_2}{c + \mu^{(q)}} [s_1^{(q)} (a + bT^{(q)}) + s_2^{(q)} (a + bL^{(q)})],$ $q \in \{1, 2, \dots, J\}$

设表2所示的所有项的集合为 Ω ， $\Pi(\Omega)$ 表示 Ω 上的齐次多项式集合。由表2可知，敌手 $\mathcal{A}$ 要想获得 $y^* = \omega^* a_0$ ，只能应用 $\Delta_0 a_0$ 和 $\{x^{(k)}, k \in \{1, 2, \dots, I\}\}$ ， $\{y^{(q)}, q \in \{1, 2, \dots, J\}\}$ 中的项，即 $y^* \in \Pi(\Delta_0 a_0, x^{(k)}, y^{(q)}, k = 1, 2, \dots, I, q = 1, 2, \dots, J)$ 。由等式(15)、式(16)可知， p_1^* 和 p_2^* 分别是 Δ_1 和 Δ_2 的倍数，故 $p_j^* \in \Pi(\Delta_j a, \Delta_j b, p_j^{(q)}, q \in \{1, 2, \dots, J\}), j = 1, 2$ 。从等式(14)、式(15)容易看出， y^* 不会含有 $\Delta_0 a_0$ 项（因为等式中所有的其他项都没有 Δ_0 ），即 $y^* \in \Pi(x^{(k)}, y^{(q)}, k = 1, 2, \dots, I, q = 1, 2, \dots, J)$ 。同理， $p_j^* (j = 1, 2)$ 不会含有单独的项 Δ_j （因为两个等式的右边只能有项 $\Delta_j \Delta_0, \Delta_j a, \Delta_j b$ ）。进而， $p_j^* (j = 1, 2)$ 也不会含有 $p_j^{(q)} (j = 1, 2)$ 项（因为会在两个等式的左边产生 $\frac{c + \mu^*}{c + \mu^{(q)}} (\mu^* \neq \mu^{(q)})$ ，而等式的右边不可能得到如此形式的项），即 $p_j^* \in \Pi(\Delta_j a, \Delta_j b), j = 1, 2$ 。由等式(15)进一步得到 y^* 不会含有 $y^{(q)}$ 项，即 $y^* \in \Pi(x^{(k)}, k = 1, 2, \dots, I)$ 。设 y^* 中包含 $x_0^{(k)}$ 项，因为等式(15)左边的项 $(c + \mu^*) p_1^*$ 不可能含有 $x^{(k)}$ ，所以将等式(15)右边的 s_1^* 分为两项，一项不含有 $x_0^{(k)}$ ，另一项含有

$\frac{x_0^{(k)}}{a + bT^*}$ ，根据等式(16)， s_2^* 也需要包含 $\frac{x_0^{(k)}}{a + bL^*}$ 项。而根据表2，敌手 $\mathcal{A}$ 只能在 $T^* = T^{(k)}$ ， $L^* = L^{(k)}$ 时能得到对应的项，这说明敌手 $\mathcal{A}$ 在密钥询问阶段得到了属性集 $\{T^*, L^*\}$ 的密钥，该签名不再是一个伪造。

3.2 安全性分析

(1) 身份和位置隐私保护

本文方案的信任管理过程中车辆发送的消息 RM_R 、 $AM_{A_i}(RM_R)$ 中包含 ABS 签名和假名，ABS 签名只与时间属性和信誉等级属性有关，不包含任何与车辆身份相关的信息。而且，在同一时间，会有大量的车辆拥有相同的信誉等级，这意味着大量的车辆具有相同的时间属性和信誉等级属性值，从而不能根据属性值对车辆进行识别。假名 PID_V 由 TA 生成，想要从假名中恢复出真实身份 RID_V ，就必须计算出 $PK_{TA}^{k_V} = g^{dk_V}$ ，只有 TA 知道私钥 d 和随机数 k_V ， $PK_{TA} = g^d$ 和 $D_{V,1} = g^{k_V}$ 公开，计算 D-H（CDH，computational Diffie-Hellman）困难问题保证除了 TA，其他方都不能在有效时间内恢复车辆的真实身份，因此，车辆的身份隐私得到保护。另外，本文方案的位置隐私指不能链接同一车辆参与的任意两次不同信誉管理的消息，因为本文方案中车辆每参与一次信誉管理，就需要更新属性私钥和假名，并且一次性假名被随机数 k_V 随机化，车辆的假名不能被链接，实现了车辆的位置隐私保护。

(2) 追踪恶意车辆

本文方案利用假名实现车辆真实身份的可追踪性。车辆 V 的假名 $PID_V = (D_{V,1}, D_{V,2}, \text{Sign}_{SK_{TA}}(D_{V,1} \parallel D_{V,2}))$ 由 TA 生成，可以实现两个目的。

① TA 不用存储假名就可以利用自己的私钥 $SK_{TA} = d$ 从假名中解析出车辆的真实身份标识 RID_V ，而且只有 TA 才能解析车辆的真实身份，保证了当合法车辆产生恶意行为时其真实身份能够被追踪。

② 假名中的签名 $\text{Sign}_{SK_{TA}}(D_{V,1} \parallel D_{V,2})$ 由 TA 利用私钥 $SK_{TA} = d$ 通过一个安全的签名算法得到，使得车辆不能自行生成不符合规则的假名，从而逃避追踪。

(3) 抵抗虚假信誉攻击

虚假信誉攻击是指车辆用一个假的信誉等级或者旧的信誉等级属性对消息签名，从而扰乱RSU对消息可信度的判断和整个信誉管理过程。例如，车辆可能倾向于利用更高的信誉等级属性获取收益。如果车辆随意选择一个假的信誉等级 $L' \in \text{TL}$ ，那么其没有相应的属性私钥，ABS签名的不可伪造性使得该车辆不能形成有效的签名。

一个可能的方法是重用以前的信誉等级属性私钥。在本文方案中，一个信誉更新过程总是取当前时隙作为时间属性，该属性值永不重复，具体体现在签名验证等式(7)、式(8)中所用的时间属性值 T_i 总是为当前时隙的值。所以车辆只能用当前自己的时间属性私钥和以前的信誉等级属性私钥对当前的消息进行签名。

根据ABS方案的定义，具有属性集 $Q(V) = \{T_i, L(V)\}$ 的车辆 V 的属性签名私钥为 $\text{SK}_V = \{K_{V,\text{base}}, K_{V,T_i} = (K_{V,\text{base}})^{1/a+bT_i}, K_0 = (K_{V,\text{base}})^{1/a_0}, K_{L(V)} = (K_{V,\text{base}})^{1/a+bL(V)}\}$ ，其中所有的私钥组件都依赖于一个公共的基底 $K_{V,\text{base}}$ ，其是群 G_1 中的一个随机生成元，在生成密钥时随机产生。因此，同一个用户在不同时隙内的属性私钥组件的基底会不相同，上述的攻击策略会导致私钥组件 K_{V,T_i} 和 $K_{L(V)}$ 的基底不相同，从而在产生的签名 σ 中 S_1 和 S_2 具有不同基底，签名验证等式(7)、式(8)不能被满足，即签名验证失败。只要划分的时隙长度使得车辆在一个时隙内只进行至多一次信誉更新，本文方案就可以防止虚假信誉攻击。

(4) 通信过程安全性

① 消息认证：由定理1可以得到没有一个多项式时间的敌手能够成功伪造消息签名。因此本文中的RSU接收到签名消息后，通过检查等式(6)~式(8)是否成立，就可以确定消息 $\sigma_R^r(m \parallel \text{TS}_R \parallel \text{PID}_R)$ 是否来自拥有合法属性私钥的合法车辆，即消息来源是否真实。并且，消息的完整性也得到保证。

② 抵抗重放攻击：车辆发送的报告消息 RM_R ，以及RSU发送的信用数据都包含了时间戳 TS_R 和 TS_{RSU} 。RSU以及TA都可以通过检查时

间戳的新鲜度来识别消息的重放。因此，本文方案能够抵御重放攻击。

4 性能分析

Liu等^[14]提出的方案中环签名采用椭圆曲线签名算法，本文方案和Chen等^[15]提出的方案采用双线性对密码。椭圆曲线密码(ECC, elliptic curve cryptosystem)设置为：群 G 是由生成元 P 生成的阶为 q 的加法群，椭圆曲线为 $y^2 = x^3 + ax + b \pmod{P}$ ，其中， P, q 为160位的素数， $a, b \in \mathbb{Z}_p^*$ 。为了便于阐述，假设本文方案中 G_1 和 G_2 是对称的，则设置双线性对为 $G_1 \times G_1 \rightarrow G_T$ 。 $\bar{P} \in G_1$ 为乘法群 G_1 中的生成元， $\bar{q}$ 为群 G_1 的阶数。本文选择效率高的Type A测试方案，构造超奇异椭圆曲线 $y^2 = x^3 + x \pmod{\bar{P}}$ ，其中 $\bar{P}$ 为512位的素数， $\bar{q}$ 为160位的素数。在Windows10系统，处理器为Intel Core i5-2400CP环境下，基于JDK1.8和JPBC-ABS2(Java pairing based cryptography)库函数来实现相关的密码运算。

4.1 计算开销

本节分析本文方案和Liu等^[14]、Chen等^[15]的方案在计算开销上的性能效率。本文只考虑V2V通信过程中车辆在本地执行的计算开销。为方便与其他方案进行定量分析与比较，本文用表3所示的密码基础操作来衡量各个方案在计算开销上的性能。其中，每个基础操作运行的时间是基于实验环境运行100次得出的平均值。

表3 密码基础操作的计算开销
Table 3 The computational cost of password based operation

密码基础操作	符号	操作含义	执行时间/ms
椭圆曲线	$\tau_{G_{bm}}$	群 G 上标量乘法操作	0.332
	$\tau_{G_{ba}}$	群 G 上加法操作	0.061
双线性对	$\tau_{G_{lbp}}$	双线性配对运算	6.698
	$\tau_{G_{lbn}}$	群 G_1 上幂运算	2.782
	$\tau_{G_{lba}}$	群 G_1 上乘法运算	0.138
哈希算法	τ_{H_1}	Hash-to-Point 哈希运算	0.031
	τ_H	SHA-1 哈希运算	0.001

3个方案的计算开销对比结果如表4所示，其中Liu等^[14]的方案中，车辆长为 l 的身份环

$(ID_1, ID_2, \dots, ID_l)$ 分别计算签名消息的组件 $(\alpha_i, \beta_i, m_i = a_i \beta_i)_{i=1, \dots, l}$, 需要执行群 G 上 $(n+2)l$ 次标量乘法运算、 nl 次加法运算、 $2l$ 次单向哈希运算和 $3l$ 次 Hash-to-Point 运算, 其中 $n = 20$ byte 表示身份 ID 的哈希输出长度, l 表示环签名中环长, 执行时间为 $(n+2)l\tau_{G_{bm}} + nl\tau_{G_{ba}} + 2l\tau_H + 3l\tau_{H-P} \approx 8.619l$ ms。在验证签名时, 需要执行群 G 上 $(n+3)l$ 次标量乘法运算、 nl 次加法运算和 $2l$ 次单向哈希运算, 执行时间为 $(n+3)l\tau_{G_{bm}} + nl\tau_{G_{ba}} + 2l\tau_H \approx 8.858l$ ms。

Chen 等^[15]的方案中使用 BBS (Boneh-Boyen-Schacham) 短群签名方案, 车辆除了签名消息时造成计算开销, 在此之前需要利用更新凭证 $rcert_i$ 验证签名私钥, 还需要执行双线性对密码群 G_1 上 2 个配对运算。车辆进行签名操作时需要执行群 G_1 上 3 次配对运算、15 次幂运算、3 次乘法运算、1 次单向哈希运算、19 次 Hash-to-Point 运算和群 G_2 上 2 次乘法运算。车辆签名时需要的计算开销为 $5\tau_{G_{1bp}} + 15\tau_{G_{1bm}} + 3\tau_{G_{1ba}} + \tau_H + 19\tau_{H-P} + 2\tau_{G_{2ba}} \approx 77.048$ ms。在验证签名的过程中, 因为在原始的 BBS 方案签名信息中加入车辆从信誉服务中心获取的信誉值 r , 所以验证计算增加了验证信誉数据的计算 $\hat{g}_{ir} = g_i \cdot k_i^r$, 该过程共需要执行双线性对密码群 G_1 上 5 次配对运算、14 次幂运算、4 次乘法运算、1 次单向哈希运算、8 次 Hash-to-Point 运算, 群 G_2 上 3 次乘法运算, 其计算开销为 $5\tau_{G_{1bp}} + 14\tau_{G_{1bm}} + 4\tau_{G_{1ba}} + \tau_H + 8\tau_{H-P} + 3\tau_{G_{2ba}} \approx 74.475$ ms。

在本文方案中, 车辆使用信誉相关的属性私钥对消息签名时, 可以提前计算组件 $(Cg^\mu)^{\hat{n}}$ 和 $(Cg^\mu)^{\hat{s}}$, 所以车辆在线计算签名还需要执行 1 次单向哈希运算、双线性密码群 G_1 上 9 次幂运算和

7 次乘法运算, 即签名计算开销为 $\tau_H + 9\tau_{G_{1bm}} + 7\tau_{G_{1ba}} \approx 26.005$ ms。验证签名阶段可以提前计算组件 Cg^μ , 另外在线验证时需要执行群 G_1 上 1 次单向哈希运算、9 次双线性对运算、5 次幂运算和 5 次乘法运算, 以及群 G_2 上 3 次乘法运算。此过程计算开销为 $\tau_H + 9\tau_{G_{1bp}} + 5\tau_{G_{1bm}} + 5\tau_{G_{1ba}} + 3\tau_{G_{2ba}} \approx 76.119$ ms。

通过表 4 比较可以得出, 本文方案基于属性签名实现车辆信誉等级的匿名验证, 相较于 Chen 等^[15]基于 BBS 短群方案, 本文方案在签名计算开销上减少了约 66.2%。由于验证计算中涉及多个双线性配对运算, 所以本文方案和 Chen 等^[15]的方案都会造成一定的验证计算开销。但本文方案中车辆属性的个数保持不变, 则签名及验证的计算开销不会随着属性个数呈线性增长。而 Liu 等^[14]的环签名方案虽然基于椭圆曲线运算, 但其签名和验证计算开销都随着身份环的环长 l 线性增长。

4.2 通信开销

本节对整个方案的通信开销进行分析, 包括系统初始化、颁发签名密钥、事件报告和信誉等级更新各个阶段的通信开销。本文选取的群 G_1 和群 G 中的元素所占字节数分别为 128 byte 和 40 byte。整数域 Z_p 和 Z_q 中的元素大小分别为 64 byte 和 20 byte。假设 VANET 中报告道路事件相关的信息、时间戳、访问结构所占字节数均为 4 byte, 另设车辆的真实身份所占字节数为 20 byte, 哈希函数的输出值大小为 20 byte, 本文方案与 Chen^[14]、Liu^[15]等方案产生的通信开销对比如表 5 所示。

由表 5 可以得出, 本文方案在系统初始化阶段和颁发签名密钥阶段的通信开销相比 Liu 等^[14]的方案较高, 但比 Chen 等^[15]方案具有更好的性能。因为在这两个阶段, Chen 等^[15]的方案会随着划分的时间间隔 d 以及信誉值的范围 s 呈线性增

表 4 计算开销对比
Table 4 Computational cost comparison

方案	签名计算	验证计算
Liu 等 ^[14] 的方案	$(n+2)l \times \tau_{G_{bm}} + nl \times \tau_{G_{ba}} + 2l\tau_H + 3l\tau_{H-P} \approx 8.619l$ ms	$(n+3)l \times \tau_{G_{bm}} + nl \times \tau_{G_{ba}} + 2l \times \tau_H \approx 8.858l$ ms
Chen 等 ^[15] 的方案	$5\tau_{G_{1bp}} + 15\tau_{G_{1bm}} + 3\tau_{G_{1ba}} + \tau_H + 19\tau_{H-P} + 2\tau_{G_{2ba}} \approx 77.048$ ms	$5\tau_{G_{1bp}} + 14\tau_{G_{1bm}} + 4\tau_{G_{1ba}} + \tau_H + 8\tau_{H-P} + 3\tau_{G_{2ba}} \approx 74.475$ ms
本文方案	$\tau_H + 9\tau_{G_{1bm}} + 7\tau_{G_{1ba}} \approx 26.005$ ms	$\tau_H + 9\tau_{G_{1bp}} + 5\tau_{G_{1bm}} + 5\tau_{G_{1ba}} + 3\tau_{G_{2ba}} \approx 76.119$ ms

长。另外，在事件报告阶段，本文方案比 Chen 等^[15]的方案生成的报告消息造成的通信开销减少了约 4.1%。在信誉更新阶段，本文方案采用在 RSU 本地计算信誉更新值，只需将信用数据反馈给 TA，大大减少了通信开销，相比 Chen 等^[15]

的方案减少约 85.9%。而 Liu 等^[14]的方案造成的通信开销会随环签名中身份环长 l 线性增长。并且在信誉更新阶段，Liu 等^[14]方案造成的通信开销与选择的评分车辆数量 t 呈线性增长的趋势。

表 5 通信开销对比
Table 5 Communication cost comparison

方案	Liu ^[14] 方案	Chen ^[15] 方案	本方案
系统初始化阶段	800 byte	$768d(s+1)$ byte	1280 byte
颁发签名密钥	60 byte	$192(d+1)$ byte	660 byte
事件报告	$110l+4$ byte	968 byte	928 byte
信誉更新	$120(t+1)+4$ byte	1104 byte	156 byte

4.3 网络仿真

由于 Chen 等^[15]的方案中并未涉及利用 RSU 参与信任管理过程，所以只对 V2V 通信过程车辆发送事件报告消息时所产生的消息时延进行了网络模拟仿真。本文利用 Veins 通信框架（它是运行车联网网络仿真的混合框架），将基于事件的网络模拟器 OMNeT++和道路交通模拟器 SUMO 连接起来建立双向通信。为了模拟 IEEE802.11p 协议下 V2V 的通信方式，从 OpenStreetMap 中截取了一段包含城区以及高速道路的道路区域作为仿真环境，导出为 OSM 文件，并利用 SUMO 中的配置工具生成道路文件 .net.xml、地形文件 .poly.xml 以及车辆行驶行为文件 .rou.xml 等文件，将其配置到 Veins 中以得到仿真的地图环境。车辆的速度为 5~30 m/s，实验仿真参数如表 6 所示。

表 6 实现仿真参数
Table 6 Experimental Simulation parameters

参数名称	值
仿真范围	$1000 \times 1000(\text{m}^2)$
模拟环境	城市街道
传输功率	20 mW
数据传输率	6 Mbit/s
车辆数量	55 辆
仿真时间	60 s

利用式(17)定义消息在发送者与接收者之间的平均消息时延 T_{Delay} 。其中， N 表示车辆的个数， m_i 表示从车辆 v_j 接收到的消息数， T_{received}^j 表示接

收到消息 m_i 的时间， T_{send}^j 表示发送的时间。

$$T_{\text{Delay}} = \frac{1}{N} \sum_{i=1}^N \left(\frac{1}{m_i} \sum_{j=1}^m (T_{\text{received}}^j - T_{\text{send}}^j) \right) \quad (17)$$

同 Liu 等^[14]、Chen 等^[15]的方案进行仿真实验对比。由表 4 和表 5 可知，Liu 等^[14]的方案生成的数据包大小，签名消息所需要的计算开销与环签名的环长大小呈线性相关。本文方案与 Liu 等^[14]的方案、Chen 等^[15]的方案产生的平均消息时延的对比结果如图 2 所示。Chen 等^[15]的方案因为数据包大小和签名计算的性能最差，所以产生的消息时延最高。实验中设定 Liu 等^[14]的方案中签名字环取值为 $l=5$ ，该方案产生的数据包大小比本文方案小，但该方案在签名计算开销上的性能会比本文方案差，由图 2 得到其产生的消息时延比本文方案高。在实际场景中，Liu 等^[14]使用环签名方案时，环长可能大于 5，所以其消息时延还会增加。另外，车辆的移动速度增大会对消息时延产生一定的影响，通过图 2 中曲线的变化可以看出增幅的趋势较缓，车辆在最大速度 30 m/s 和最低速度 5 m/s 产生的消息时延相比不超过 0.005 s，说明车辆在高速移动中，消息时延也可以保持较小的变化，仿真结果进一步验证了本文方案的性能。

5 结束语

针对车联网信任管理中的隐私问题，本文利用属性签名设计了一种匿名的信任管理方案。基于属性签名具有的匿名性和选定的特殊访问结构

使得车辆在信任管理过程中的身份和位置隐私得到保护。信誉等级属性的应用使得信任管理过程中无须在 TA 处查询车辆的信誉等级, 消息签名的验证过程实现了车辆信誉等级的匿名验证。时间属性的应用使得车辆必须应用最新的信誉等级值, 防止信誉值的滥用造成信任管理失效。和已有方案相比, 虽然本文方案所用的属性签名验证带来一定的计算开销, 但通信没有明显增强且具有更强的隐私保护。带有签名的假名机制实现车辆身份的合法和安全追踪并防御车辆生成不符合规范的假名以逃避合法追踪。未来进一步的工作是探索车联网环境下分布式的信任管理机制, 避免单一信任管理中心带来的负面影响。

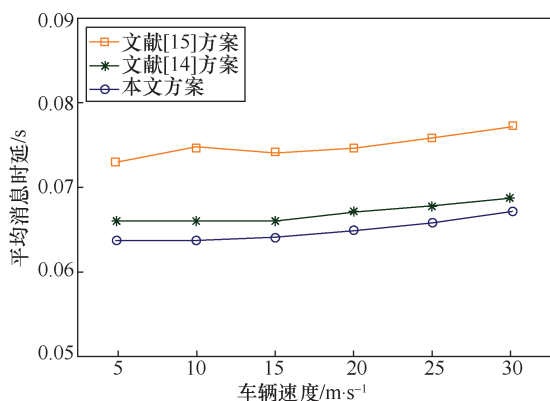


图2 平均消息时延与车辆速度的关系

Figure 2 Average message latency in relation to vehicle speed

参考文献:

- [1] LU Z J, QU G, LIU Z L. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(2): 760-776.
- [2] ZHANG J. Trust management for VANETs: challenges, desired properties and future directions[J]. International Journal of Distributed Systems and Technologies, 2012, 3(1): 48-62.
- [3] KERRACHE C A, CALAFATE C T, CANO J, et al. Trust management for vehicular networks: an adversary-oriented overview[J]. IEEE Access, 2016, 4: 9293-9307.
- [4] HBAIEB A, AYED S, CHAARI L. A survey of trust management in the Internet of Vehicles[J]. Computer Networks, 2022, 203: 108558.
- [5] HUSSAIN R, LEE J, ZEADALLY S. Trust in VANET: a survey of current solutions and future research opportunities[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(5): 2553-2571.
- [6] 刘雪艳, 王力, 邹丽娟, 等. 车联网环境下无证书匿名认证方案[J]. 电子与信息学报, 2022, 44(1): 295-304.
- [7] LIU X Y, WANG L, HUAN L J, et al. Certificateless anonymous authentication scheme for internet of vehicles[J]. Journal of Electronics & Information Technology, 2022, 44(1): 295-304.
- [8] JAIMES L M S, ULLAH K, MOREIRA E D S. ARS: anonymous reputation system for vehicular ad hoc networks[C]//Proceedings of The 8th IEEE Latin-American Conference on Communications (LATINCOM). 2016: 1-6.
- [9] TANGADE S, MANVI S S, LORENZ P. Trust management scheme based on hybrid cryptography for secure communications in VANETs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5232-5243.
- [10] LI Z M, CHI G C. On joint privacy and reputation assurance for vehicular ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(10): 2334-2344.
- [11] WANG S B, YAO N M. A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs[J]. Wireless Networks, 2019, 25(3): 1099-1115.
- [12] BEHZAD D, FARZANEH N. A novel trust management method to preserve privacy in vehicular ad-hoc networks[J]. Peer-to-Peer Networking and Applications, 2021, 14: 1118-1131.
- [13] YAN X M, GU X, WANG J, et al. A kind of event trust model for VANET based on statistical method[J]. Wireless Personal Communications, 2021, 118: 489-503.
- [14] JUNEJO M H, RAHMAN A, SHAIKH R A, et al. A privacy-preserving attack-resistant trust model for Internet of vehicles ad hoc networks[J]. Scientific Programming, 2020, 2020(2): 1-21.
- [15] LIU X C, HUANG H P, XIAO F, et al. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs[J]. IEEE Internet of Things Journal, 2020, 7(5): 4101-4112.
- [16] CHEN L Q, LI Q, MARTIN K M, et al. Private reputation retrieval in public-a privacy-aware announcement scheme for VANETs[J]. Iet Information Security, 2017, 11(4): 204-210.
- [17] HASROUNY H, SAMHAT A E, BASSIL C, et al. Trust model for secure group leader-based communications in VANET[J]. Wireless Networks, 2019, 25: 4639-4661.
- [18] 常朝稳, 金建树, 韩培胜, 等. 基于属性签名标识的 SDN 数据包转发验证方案[J]. 通信学报, 2021, 42(6): 131-144.
- [19] CHANG C W, JIN J S, HAN P S, et al. Software-defined network packet forwarding verification scheme based on attribute-based signatures identification[J]. Journal on Communications, 2021, 42(6): 131-144.
- [20] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[J]. IACR Cryptology ePrint Archive, 2008: 328.
- [21] KIM C, BAE I. A misbehavior-based reputation management system for VANETs[J]. Embedded and Multimedia Computing Technology and Service, 2012, 181: 441-450.
- [22] LU Z J, LIU W C, WANG Q, et al. A privacy-preserving trust model based on blockchain for VANETs[J]. IEEE Access, 2018, 6: 1.

[作者简介]



肖敏（1971- ），女，湖北宜昌人，重庆邮电大学教授，主要研究方向为现代密码学理论与应用、车联网安全、量子密码。



黄永洪（1974- ），男，重庆人，重庆邮电大学讲师，主要研究方向为安全操作系统、人工智能安全。



毛发英（1996- ），女，贵州兴义人，重庆邮电大学硕士生，主要研究方向为现代密码学理论与应用、车联网安全。



曹云飞（1968- ），男，四川成都人，中国电子科技网络信息安全有限公司研究员，主要研究方向为密码基础理论和信息安全技术。