文章编号:1007-5321(2020)01-0104-07 **DOI**:10.13190/j.jbupt.2019-017

一种车载网隐私保护方案的分析与改进

李 涛[1,2], 张 静[3], 杨 皓[2]
(1. 九江学院 认知科学与跨学科研究中心, 九江 332005; 2. 九江学院 理学院, 九江 332005;
3. 九江学院 信息科学与技术学院, 九江 332005)

摘要: 从安全性角度对一种车载网隐私保护方案进行了研究,指出该方案存在无法抵抗共谋攻击的问题,对该方案进行改进,提出了新的车载网隐私保护方案,解决了车载网的隐私保护、匿名性、共谋攻击、重放攻击等多种安全问题. 与现有的车载网隐私保护方案相比,新方案提高了安全性.

关 键 词: 车载自组织网络; 隐私保护; 匿名认证; 安全多方计算
中图分类号: TP309 **文献标志码**: A

Analysis and Improvement of Privacy Protection Scheme in VANET

LI Tao[1,2], ZHANG Jing[3], YANG Hao[2]
(1. Cognitive Scienceand Interdisciplinary Research Center, Jiujiang University, Jiujiang 332005, China;
2. School of Information Science and Technology, Jiujiang University, Jiujiang 332005, China;
3. College of Science, Jiujiang University, Jiujiang 332005, China)

Abstract: Through analysis a privacy protection scheme in vehicle Ad hoc network (VANET), it is revealed that the scheme cannot resist the collusion attack. Based on the scheme, a novel privacy protection scheme is proposed. It is proved that the proposed scheme solves privacy protection, anonymity, collusion attack, replay attack, etc. Compared with current privacy protection schemes in VANET, the novel scheme is more security.

Key words: vehicular Ad hoc network; privacy protection; anonymous authentication; security multiparty computation

车载自组织网络[1](VANET, vehicle Ad hoc network)是移动自组织网络(MANET, mobile Ad hoc network)在交通道路上的拓展应用,以车辆单元为主要通信节点,自组织成一个通信网络. 融合了机动车辆和无线自组织网络的特点,与一般的移动自组织网络不同,车载自组织网络具有网络拓扑结构高速动态变化、网络负荷变化等显著特征. 车载自组织网络一般由车辆子网、服务基础设施、网络运营商 3 部分组成. 其中车辆子网是由机动车辆上配置的车载通信单元(OBU, on-board unit)通过无线网络连接而成. 服务基础设施包括有权威的认证中心(CA, certificate authority)、路侧单元(RSU, road side unit)和服务提供商(SP, service provider). 网络运营商即是提供基础通信服务的互联网服务提供商.

在车载自组织网络中,一般包含 2 种通信,分别

收稿日期: 2019-01-24
基金项目: 国家自然科学基金项目(61462048); 2017 年教育部产学研合作协同育人项目(201702092002, 201702178034, 201702139065, 201701024020, 201701044078); 2017 年江西省社会科学规划项目(17xw08); 2019 年江西省高等学校教学教改研究重点课题(JXJG-19-17-1); 九江学院 2019 年度校级教改课题(XJJGZD-19-06)
作者简介: 李 涛(1979—), 男, 副教授, E-mail: 664723267@qq.com.

为车与车(V2V, vehicle to vehicle)通信和车与基础设施(V2I, vehicle to infrastructure)通信. V2V 和 V2I 都是通过无线网络通信,RSU 与骨干网络的通信则是通过有线网络. 系统网络架构模型如图 1 所示.

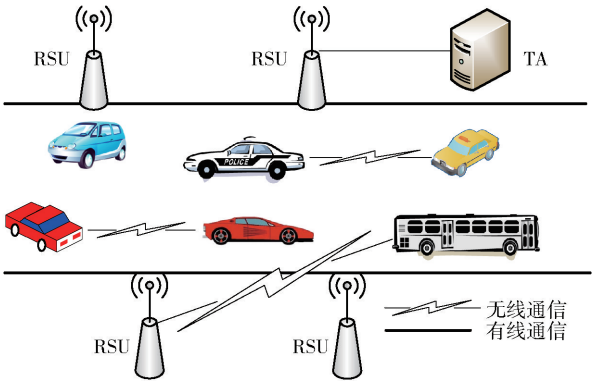

图 1　VANET 模型

车载自组织网络中车辆节点接受基于位置的服务(LBS, location based services),一般可分为安全类服务和增值类服务 2 类. 安全类服务指的是在车辆子网中车辆节点通过相互交换各自的车速、实时位置、当前路况等信息,以此达到避免交通事故,提高道路通行效率等目的;增值类服务主要是为了满足乘客在车载环境中的办公、娱乐等需求,如车载环境中的数据上传与下载、电子广告等. 因为 LBS 提供的服务与用户提出服务申请的位置有关[2],所以用户在使用相关服务的过程中有位置隐私泄露的风险.

为防止位置隐私泄露,在享受相关服务时使用假名方案是实现位置隐私保护的重要方法之一. Raya 等[3]首次提出了一种基于假名证书的车载网匿名认证协议,使用假名证书来隐藏车辆的真实信息,基本实现了用户的隐私保护. 但是该方案在假名存储分发和撤销方面有着较大的性能开销. 另外,因为证书中心集中授权分发车辆证书,所以也存在瓶颈问题. Bellur[4]提出的方案采用分布式的假名管理. 该方案中车辆节点只需要从 RSU 处获得假名证书,每个 RSU 负责某个区域的证书颁发. 该方案的优点是假名的分发和撤销效率较高,证书颁发更加灵活可控. 但在该方案中 RSU 的分布位置和密度是研究的重点与难点. Papadimitratos 等[5]提出基于群签名算法实现车载网隐私保护,该方案中车辆节点使用群签名算法计算生成临时的公钥基础设施(PKI, public key infrastructure)证书,之后使用 PKI 证书签发与其他节点的通信数据. 该方案在一定程度上降低了节点身份认证的性能开销,不足之处在于撤销恶意节点的开销还是较大. Sundari 等[6]提出应用安全多方计算,在差异化私有数据中实现数据完整性保护的方案,安全可靠地实现了输出数据在不同输入方之间进行分配. Lin 等[7]提出了一种基于群签名和基于身份签名的车载自组织网络匿名认证方案,并证明方案实现了一定的隐私性保护. 该方案在 V2V 通信中使用群签名来保证消息的不可关联性,并基于身份签名来降低 V2I 的通信开销. 但此方案的不足在于,该协议不能实时地从车载自组织网系统中撤销具有不良记录的恶意节点的身份标识. Guo 等[8]和 Sun 等[9]基于群签名算法也提出了类似方案. 基于群签名算法的方案一般存在签名长度过长,身份验证和身份撤销开销较大的弱点. Zeng 等[10]提出基于条件匿名环签名方案,该方案可以合理高效地控制匿名性. 但该方案的消息身份认证所需时间随证书更新列表呈线性增长. Shao 等[11]提出一种具有阈值认证特点的群签名认证方案. 现有的典型方案大都是基于非对称密码机制来设计的,存在效率较低的问题. 安全多方计算[12]在解决隐私保护问题方面具有明显优势,宋成等[13]基于线性方程组求解理论[14]和安全多方计算[12],提出了一种基于安全多方计算的车载网隐私保护机制,有效解决了车载网匿名认证过程中的计算瓶颈问题. 经分析发现,该方案在身份认证过程中存在安全漏洞. 笔者从增强安全性的角度上,针对性地提出一些改进措施,以弥补该漏洞. 在文献[13]方案的基础上,新方案解决了车载网的隐私保护、匿名性、共谋攻击、重放攻击等多种安全问题.

1　相关知识

1.1　符号说明

本方案中使用相关符号含义如表 1 所示.

1.2　线性方程组求解理论[15]

定理 1　n 元线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 有解的充分必要条件是系数矩阵 $\boldsymbol{A}$ 的秩等于增广矩阵 $\boldsymbol{B}=(\boldsymbol{A},\boldsymbol{b})$ 的秩,即 $R(\boldsymbol{A})=R(\boldsymbol{B})$.

定理 2　若 n 元线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 有解,如果 $R(\boldsymbol{A})=n$,那么方程组有唯一解;如果 $R(\boldsymbol{A})<n$,那么方程组有无穷多解.

定理 3　设 $\boldsymbol{x}_1=\boldsymbol{\eta}_1$ 及 $\boldsymbol{x}_2=\boldsymbol{\eta}_2$ 是非齐次线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 的解,则 $\boldsymbol{x}=\boldsymbol{\eta}_1-\boldsymbol{\eta}_2$ 为对应的齐次线性

表1 相关符号

符号	含义
G	阶为 q 的乘法循环群
g,h	循环群 G 上的生成元
Y_1,Y_2	DDH 问题的 2 个分布
R_s	路侧单元节点
V_p	车辆节点
H	哈希函数
$\boldsymbol{A}$	$m\times n$ 矩阵
$\boldsymbol{y}$	m 维列向量
$\boldsymbol{x}$	n 维列向量
$\boldsymbol{D}_i$	第 i 个 $m\times n$ 矩阵
$\boldsymbol{m}_t$	V_p 拥有的 t 个消息
$\boldsymbol{\delta}_i$	R_s 选择的 i 个消息
id	方程组 $\boldsymbol{Ax}=\boldsymbol{y}$ 的一个解对应的 id 值

方程组 $Ax=0$ 的解.

定理4 设 $\boldsymbol{x}_1=\boldsymbol{\eta}$ 是非齐次线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 的解,$\boldsymbol{x}_2=\boldsymbol{\xi}$ 是对应齐次线性方程组 $\boldsymbol{Ax}=0$ 的解,则 $\boldsymbol{x}=\boldsymbol{\xi}+\boldsymbol{\eta}$ 仍是线性方程组 $\boldsymbol{Ax}=\boldsymbol{b}$ 的解.

定理5 若 $\boldsymbol{x}=\boldsymbol{\xi}_1$ 是齐次线性方程组 $\boldsymbol{Ax}=0$ 的解,k 为实数,则 $\boldsymbol{x}=k\boldsymbol{\xi}_1$ 也是线性方程组 $\boldsymbol{Ax}=0$ 的解.

1.3 茫然传输协议

茫然传输协议[16](OT,oblivious transfer)是一个重要的密码学原语,它可以被应用到许多密码学协议的构造中,特别是它在隐私保护的数据查询、安全多方计算等多个领域中有着重要的应用.

茫然传输协议[16]一般分为2个参与方:发送方 S 和接收方 R,协议的目的是让接收方从发送方的输入中获取自己选择的输入,且满足:

1)发送方不知道接收方的选择;

2)接收方只能获得自己选择的输入且无法获得额外的输入信息.

茫然传输协议的安全性基础是基于判定性 Diffie-Hellman(DDH, decisional Diffie-Hellman)问题.

DDH[17-18]问题:给定素数 q 和 Z_q^* 中2个独立的生成元 g 以及 g^α、g^β、g^γ,判定 $g^\gamma\stackrel{?}{=}g^\alpha g^\beta$,其中 $g\in G_1$,α、β、$\gamma\in Z_q^*$ 为任意未知整数.

2 方案的具体实现

宋成等[13]提出的基于安全多方计算的车载网隐私保护方案主要包含3个阶段,分别为注册阶段、认证阶段和更新阶段. 注册阶段完成车辆节点 V_p 和路侧单元节点 R_s 在可信服务中心(TA,trusted center)处的注册登记. 认证阶段实现 R_s 对 V_p 的匿名认证. 更新阶段则是在车载网中有车辆节点进入或退出时,V_p 和 R_s 定期到TA处更新系统认证信息.

1)注册阶段

系统进行初始化,设定公共参数. TA随机生成一个 $m\times n$ 维的矩阵 $\boldsymbol{A}(2\leqslant m\leqslant n)$ 和一个 m 维列向量 $\boldsymbol{y}$,且满足 $R(\boldsymbol{A})=R(\boldsymbol{A},\boldsymbol{y})<n$,即线性方程组 $\boldsymbol{Ax}=\boldsymbol{y}$ 有无穷多解. TA为车辆子网中每个车辆节点生成特定的 n 维向量 $\boldsymbol{x}_i$,$\boldsymbol{x}_i$ 满足 $\boldsymbol{Ax}_i=\boldsymbol{y}$,即 $\boldsymbol{x}_i$ 为线性方程组 $\boldsymbol{Ax}=\boldsymbol{y}$ 的某个解. 然后TA将向量 $\boldsymbol{x}_i$ 发送给相应车辆节点 V_P 作为其合法身份标识. TA再将认证矩阵 $\boldsymbol{A}$ 和认证向量 $\boldsymbol{y}$ 通过安全信道发送给系统中每个 R_S 节点作为身份认证信息.

2)认证阶段

当 V_p 进入某个 R_s 区域需要进行通信时,首先要完成身份认证. V_p 向 R_s 发送身份认证请求,R_s 判断其是否为合法用户.

① V_p 向 R_S 发送身份认证请求,V_P 随机选择乘法循环群 G 的2个生成元 g,h,并将 (g,h) 发送给 R_s.

② R_s 收到车辆节点的身份认证请求之后,从集合 Z_q 中随机选择一个数 k,再生成 k 个随机矩阵 $\boldsymbol{D}_1,\boldsymbol{D}_2,\cdots,\boldsymbol{D}_k$,且满足 $\boldsymbol{A}=\boldsymbol{D}_1+\boldsymbol{D}_2+\cdots+\boldsymbol{D}_k$. 然后,$R_S$ 生成一个秘密随机数 t,且满足 $t>k$,R_s 再生成 t 个矩阵 $(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$,并将其发送给 V_p,其中 $(\boldsymbol{D}_1,\boldsymbol{D}_2,\cdots,\boldsymbol{D}_k)\subset(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$,且 $\boldsymbol{H}_i=\boldsymbol{D}_j$(这里 i 与 j 是随机的). 在 $(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$ 中,除 $\boldsymbol{H}_i$ 外,其余的均为随机矩阵.

③ 对所有的 $i=1,2,\cdots,t$,V_P 生成随机向量 $\boldsymbol{r}_j$ 并计算 $\boldsymbol{H}_i\boldsymbol{x}+\boldsymbol{r}_j$,计算后 V_P 则拥有了 t 个消息,记做 $\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_t$. 其中 $\boldsymbol{m}_1=\boldsymbol{H}_1\boldsymbol{x}+\boldsymbol{r}_1$,$\boldsymbol{m}_2=\boldsymbol{H}_2\boldsymbol{x}+\boldsymbol{r}_2$,$\cdots$,$\boldsymbol{m}_t=\boldsymbol{H}_t\boldsymbol{x}+\boldsymbol{r}_t$. $(\delta_1,\delta_2,\cdots,\delta_k)\subset(1,2,\cdots,t)$ 表示 R_s 选择其中的 k 个消息,记做 $\boldsymbol{m}_{\delta_1},\boldsymbol{m}_{\delta_2},\cdots,\boldsymbol{m}_{\delta_k}$. 利用茫然传输协议,$R_s$ 取回结果 $\boldsymbol{H}_i\boldsymbol{x}+\boldsymbol{r}_j=\boldsymbol{D}_j\boldsymbol{x}+\boldsymbol{r}_j$. 接着如下计算:

R_s 首先计算

$$f'(x)=(x-\delta_1)(x-\delta_2)\cdots(x-\delta_k)=b_0+b_1x+\cdots+x^k$$

接着,随机选择一个多项式:

$$f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}+x^k$$

然后再随机选取 $a_i\in Z_q(0\leqslant i\leqslant k)$,并计算

$$A_0 = g^{a_0} h^{b_0} \bmod p$$

$$A_1 = g^{a_1} h^{b_1} \bmod p, \cdots, A_{k-1} = g^{a_{k-1}} h^{b_{k-1}} \bmod p$$

最后，R_s 发送给 V_p. 随后，V_p 首先从集合 Z_q 中随机选择一个数 l，并计算

$$B_i = g^{lf(i)} h^{lf'(i)} = (A_0 A_1^i A_2^{i^2} A_{k-1}^{i^{k-1}} (gh)^{i^k})^l \bmod p$$

$$\boldsymbol{C}_i = \boldsymbol{m}_i B_i \bmod p$$

$$\boldsymbol{r} = \sum_{j=1}^{k} \boldsymbol{r}_j$$

其中 $i = 1, 2, \cdots, t$，然后发送 $(\boldsymbol{r}, g^l, \boldsymbol{C}_1, \cdots, \boldsymbol{C}_t)$ 给 R_s.

对于 $i = \delta_1, \delta_2, \cdots, \delta_k$，$R_s$ 计算：

$$\boldsymbol{m}'_{\delta_i} = \boldsymbol{C}_{\delta_i} ((g^l)^{f(\delta_i)})^{-1}$$

其中　　$((g^l)^{f(\delta_i)})^{-1} (g^l)^{f(\delta_i)} = 1 \bmod p$

此时，$(\boldsymbol{m}'_{\delta_1}, \boldsymbol{m}'_{\delta_2}, \cdots, \boldsymbol{m}'_{\delta_k})$ 正是 R_s 所选择的 k 个消息 $\boldsymbol{H}_i \boldsymbol{x} + \boldsymbol{r}_j = \boldsymbol{D}_j + \boldsymbol{r}_j$，其中 $i = 1, 2, \cdots, k$.

④ R_s 计算：

$$\boldsymbol{W} = \sum_{j=1}^{t} \boldsymbol{D}_j x + \sum_{j=1}^{t} \boldsymbol{r}_j = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{r}$$

$$\boldsymbol{y}' = \boldsymbol{W} - \boldsymbol{r} = \boldsymbol{A}\boldsymbol{x}$$

若 $\boldsymbol{y} = \boldsymbol{y}'$ 则认证通过，否则拒绝该认证消息.

3）更新阶段

由方程组

$$\left.\begin{aligned} \boldsymbol{A}\boldsymbol{x}_1 &= \boldsymbol{y} \\ \boldsymbol{A}\boldsymbol{x}_2 &= \boldsymbol{y} \\ &\vdots \\ \boldsymbol{A}\boldsymbol{x}_n &= \boldsymbol{y} \end{aligned}\right\}$$

当 $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n$ 已知时，可求 $\boldsymbol{A}$ 和 $\boldsymbol{y}$. 其中，$\boldsymbol{A}$ 是 $m \times n$ 阶矩阵，$\boldsymbol{y}$ 是 m 维列向量. 在车载自组织网中，若有新车辆节点的加入或退出，可以利用现有节点 $\boldsymbol{x}$，由服务器重新计算认证矩阵 $\boldsymbol{A}$ 和认证向量 $\boldsymbol{y}$ 的一个解，并作为相关认证信息发送给路侧单元 R_s.

3　对方案的攻击

在文献[13]中的方案中，认证阶段和更新阶段存在漏洞，防合谋攻击的证明中也存在安全漏洞. 仔细分析合谋攻击的安全证明后，发现合谋攻击的恶意节点确实无法解出秘密认证矩阵 $\boldsymbol{A}$ 与认证向量 $\boldsymbol{y}$，但基于线性方程组的相关求解理论，上述证明的漏洞在于系统中发起合谋攻击的恶意节点不用知晓秘密认证矩阵 $\boldsymbol{A}$ 与认证向量 $\boldsymbol{y}$ 就可以得到无穷多的满足方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的解，即可以得到无穷多的合法身份标识. 恶意节点的合谋攻击会影响系统的认证阶段和更新阶段，破坏系统的身份认证过程，攻击方法如下.

以 2 个成员合谋攻击为例，假设合谋攻击成员甲的合法身份标识为 $\boldsymbol{\eta}_1$，合谋攻击成员乙的合法身份标识为 $\boldsymbol{\eta}_2$，显然 $\boldsymbol{\eta}_1$ 与 $\boldsymbol{\eta}_2$ 都为线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的解.

令 $\boldsymbol{\xi} = \boldsymbol{\eta}_1 - \boldsymbol{\eta}_2$，根据定理 3 得到

$$\boldsymbol{A}\boldsymbol{\xi} = \boldsymbol{A}(\boldsymbol{\eta}_1 - \boldsymbol{\eta}_2) = \boldsymbol{A}\boldsymbol{\eta}_1 - \boldsymbol{A}\boldsymbol{\eta}_2 = \boldsymbol{y} - \boldsymbol{y} = 0$$

故 $\boldsymbol{\xi}$ 为对应的齐次线性方程组 $\boldsymbol{A}\boldsymbol{x} = 0$ 的解.

令 $\boldsymbol{\omega} = \boldsymbol{\eta}_1 + \boldsymbol{\xi}$，根据定理 4 得到

$$\boldsymbol{A}\boldsymbol{\omega} = \boldsymbol{A}(\boldsymbol{\eta}_1 + \boldsymbol{\xi}) = \boldsymbol{A}\boldsymbol{\eta}_1 + \boldsymbol{A}\boldsymbol{\xi} = \boldsymbol{y} + 0 = \boldsymbol{y}$$

故 $\boldsymbol{\omega}$ 为非齐次线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的解.

令 $\boldsymbol{\zeta} = \boldsymbol{\eta}_1 + k\boldsymbol{\xi}$，$(k \in R)$，根据定理 4 和定理 5 得到

$$\boldsymbol{A}\boldsymbol{\zeta} = \boldsymbol{A}(\boldsymbol{\eta}_1 + k\boldsymbol{\xi}) = \boldsymbol{A}\boldsymbol{\eta}_1 + \boldsymbol{A}k\boldsymbol{\xi} = \boldsymbol{y} + 0 = \boldsymbol{y}$$

故 $\boldsymbol{\zeta}$ 也为线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的解. 其中 k 可以取任意的实数. 攻击者由此可以获得无穷多的线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的解，即可以获得无穷多的合法身份标识. 显然，这意味着攻击者的合谋攻击成功了.

4　改进的方案

分析认为车辆在注册阶段不能仅仅以线性方程组的一个解作为合法身份标识，因为有可能会导致遭受合谋攻击. 由于哈希函数具有易计算、单向性和抗碰撞性等优良特性. 为提高方案安全性，在改进方案中引入哈希函数，同时修正原方案存在的错误.

1）注册阶段

① TA 随机生成一个 $m \times n$ 维的矩阵 $\boldsymbol{A}$ $(2 \leqslant m \leqslant n)$ 和一个 m 维的列向量 $\boldsymbol{y}$，且满足 $R(\boldsymbol{A}) = R(\boldsymbol{A}, \boldsymbol{y}) < n$，即线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 有无穷多解.

② 系统中每注册一个节点，注册服务器就计算出线性方程组 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}$ 的一个解 $\boldsymbol{x}_i$，同时注册服务器给该“解”设定一个随机且唯一的 id 值. 并以此生成并维护一张数据表，记录方程组的解与 id 值，表中每一个解与 id 值是一一对应的关系. 当有节点的加入或退出时更新数据表.

③ 系统选择 SHA 作为哈希函数 H，为 SHA 设定好相关公共参数后，输入 id 值，计算出 $H(\mathrm{id})$.

④ 构造二元组 $(\boldsymbol{x}_i, H(\mathrm{id}))$ 作为车辆节点的身份标识，TA 通过安全信道将 $(\boldsymbol{x}_i, H(\mathrm{id}))$ 发送给相应车辆节点 V_p，然后将矩阵 $\boldsymbol{A}$、认证向量 $\boldsymbol{y}$、数据表发送给每个 R_s 节点作为系统认证信息.

2）认证阶段

当 V_p 要进行通信时，必须先进行身份认证. V_p

向 R_s 发送身份认证请求，R_s 对其进行身份认证.

① V_P 随机选择循环群 G 的2个生成元 g,h，并将(g,h)和$(\boldsymbol{x}_i,H(\mathrm{id}))$发送给 R_s.

② R_s 收到车辆节点的认证请求之后，从集合 Z_q 中随机选择一个数 k，再生成 k 个随机矩阵 $\boldsymbol{D}_1,\boldsymbol{D}_2,\cdots,\boldsymbol{D}_k$，且满足 $\boldsymbol{A}=\boldsymbol{D}_1+\boldsymbol{D}_2+\cdots+\boldsymbol{D}_k$. R_S 生成一个秘密随机数 t，且满足 $t>k$，R_s 再生成 t 个 $m\times n$ 维矩阵$(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$，且$(\boldsymbol{D}_1,\boldsymbol{D}_2,\cdots,\boldsymbol{D}_k)\subset(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$，在$(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$中 $\boldsymbol{H}_i=\boldsymbol{D}_j,i=1,2,\cdots,t.\ j=1,2,\cdots,k$，这里的 i 与 j 是随机的. 其余 $t-k$ 个矩阵 $\boldsymbol{H}$ 是 $m\times n$ 维的随机矩阵，然后 R_s 将$(\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_t)$发送给 V_p.

③ 对所有的 $i=1,2,\cdots,t$，V_P 生成随机向量 $\boldsymbol{r}_j$，并计算 $\boldsymbol{H}_t\boldsymbol{x}+\boldsymbol{r}_j$. V_P 拥有了 t 个消息，记做 $\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_t$. 其中 $\boldsymbol{m}_1=\boldsymbol{H}_1\boldsymbol{x}+\boldsymbol{r}_1$，$\boldsymbol{m}_2=\boldsymbol{H}_2\boldsymbol{x}+\boldsymbol{r}_2,\cdots,\boldsymbol{m}_t=\boldsymbol{H}_t\boldsymbol{x}+\boldsymbol{r}_t$，然后 V_P 将$(\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_t)$发送给 R_s. R_s 根据

$$\boldsymbol{m}_{\delta_n}=\boldsymbol{H}_t\boldsymbol{x}+\boldsymbol{r}_j=\boldsymbol{D}_j\boldsymbol{x}+\boldsymbol{r}_j,\ n=1,2,\cdots,k,$$
$$i=1,2,\cdots,t,\ j=1,2,\cdots,k$$

利用茫然传输协议选择性地取回其中的 k 个消息，记做 $\boldsymbol{m}_{\delta_1},\boldsymbol{m}_{\delta_2},\cdots,\boldsymbol{m}_{\delta_k}$.

④ R_s 根据 $\boldsymbol{x}_i$ 和数据表计算出对应的 id′值，使用哈希函数 H 计算 $H(\mathrm{id}')$值. 再计算

$$\boldsymbol{W}=\sum_{j=1}^{t}\boldsymbol{H}_jx+\sum_{j=1}^{k}\boldsymbol{r}_j=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{r}$$
$$\boldsymbol{y}'=\boldsymbol{W}-\boldsymbol{r}=\boldsymbol{A}\boldsymbol{x}$$

若 $H(\mathrm{id})=H(\mathrm{id}')$，且 $\boldsymbol{y}=\boldsymbol{y}'$，则认证通过；否则，认证失败.

3）更新阶段

R_s 根据矩阵 $\boldsymbol{A}$ 和向量 $\boldsymbol{y}$ 计算出线性方程组 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{y}$ 的一个解 $\boldsymbol{x}_i$ 后，注册服务器同时给该“解”设定一个随机且唯一的 id 值，将二元组$(\boldsymbol{x}_i,H(\mathrm{id}))$作为身份标识发给车辆节点 V_p.

5 改进方案安全性分析

5.1 安全说明

1）合谋攻击

以线性方程组 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{y}$ 的解和数据表中对应 id 的哈希值为元素，构造二元组$(\boldsymbol{x}_i,H(\mathrm{id}))$作为车辆节点的合法身份标识. 在验证车辆节点身份时，同时满足 $H(\mathrm{id})=H(\mathrm{id}')$和 $\boldsymbol{y}=\boldsymbol{y}'$才能认证通过，所以合谋攻击者虽然获取了无穷多的线性方程组 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{y}$ 的解，但无法获得合法 $H(\mathrm{id})$值，所以攻击者将不能顺利通过身份验证，即合谋攻击不能以不可忽略的概率攻击成功.

2）接收者隐私

对于任意不同的$(\delta_1',\delta_2',\cdots,\delta_k')$，都会确定一个 k 阶多项式 $f_1'(x)=(x-\delta_1')(x-\delta_2')\cdots(x-\delta_k')=b_0'+b_1'x+b_2'x^2+\cdots+x_k$，且存在一个 k 阶多项式 $f_1(x)=a_0'+a_1'x+a_2'x^2+\cdots+a_{k-1}'x^{k-1}+x^k$，满足$A_i=g^{a_i'}h^{b_i'}(0\leqslant i\leqslant k-1)$，所以根据接收者 R_s 发出的消息，A_i 并不能获得 R_s 所选择的特定消息，即接收者 R_s 的隐私可以达到无条件安全. 此过程中，考虑到碰撞攻击，V_p 猜对接收者所选择消息的概率是 $1/C_t^k$，此概率和 k、t 相关. 假设当发送者 V_p 成功实现碰撞攻击时，根据 $\boldsymbol{W}=\sum_{j=1}^{t}\boldsymbol{H}_jx+\sum_{j=1}^{k}\boldsymbol{r}_j=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{r}$ 可知，$\boldsymbol{r}_j$是由 V_p 随机生成的，所以 V_p 通过已知的 $\boldsymbol{W},\boldsymbol{r},\boldsymbol{x}$ 求解 $\boldsymbol{A}$，则 $\boldsymbol{A}$ 有无穷多个解，V_p 不能从中选出 R_s 所使用的 $\boldsymbol{A}$. 显然，接收者 R_s 隐私是安全的.

对于发送者隐私、匿名性以及重放攻击的安全证明与文献[13]方案一致，故略去.

由于笔者的主要工作表现在提高方案的安全性上面，故下面进行改进方案与其他的典型方案安全性对比，如表2所示.

表2 安全性比较

安全性	文献[7]	文献[10]	文献[11]	文献[13]	本文方案
V_p 隐私	实现	实现	实现	实现	实现
R_s 隐私	实现			实现	实现
匿名性	实现	实现	实现	实现	实现
抗合谋攻击					实现
抗重放攻击				实现	实现

5.2 效率分析

下面分析改进方案与文献[13]方案在效率方面的差异.

文献[13]中的方案把线性方程组的解作为车辆节点的身份标识，而改进方案以线性方程组某个解和对应 id 的哈希值构成的二元组作为车辆节点的身份标识. 在改进方案的注册阶段增加了2项操作，分别是计算一次解对应 id 的哈希值和生成维护相关数据表. 由于哈希函数具有易计算的特性，对如今的车载计算芯片来说，这个过程的计算开销相比其他的计算任务几乎可忽略不计. 另外，在生成需要维护的数据表时，设备所产生的性能开销，因车

载自组织网络的自身特性，在应用中每个 R_s 节点需要维护的数据表通常不大，现有的车载计算芯片对此过程的性能开销同样非常小.

改进方案在认证更新阶段与文献[13]方案相比增加了一项操作，计算出解对应 id 的哈希值，并与二元组中的哈希值进行比对. 这个过程的性能开销也是远小于其他计算过程.

综上可知，改进方案与文献[13]方案相比，在各个阶段虽然增加了几项操作，但增加的操作所产生的性能开销几乎可忽略不计. 所以在一定程度上，可以认为改进方案在增强安全性的基础上计算效率略有下降. 性能开销对比如表 3 所示.

表 3　计算总开销比较

方案	计算总开销
文献[13]	$(3m+4k)T_{\text{mul}}+(2m+4k-2)T_{\text{exp}}+kT_{\text{in}}$
本文方案	$(3m+4k)T_{\text{mul}}+(2m+4k-2)T_{\text{exp}}+kT_{\text{in}}+2T_{\text{h}}$

5.3　方案安全性及效率综合分析

6.1 和 6.2 节中只进行了改进方案的安全及效率分析，存在一定的片面性，这里主要综合分析改进方案和相关车载自组网方案.

表 4　方案安全性及效率综合分析

安全性	文献[7]	文献[10]	文献[11]	文献[13]	本文方案
V_p 隐私	实现	实现	实现	实现	实现
R_s 隐私	实现			实现	实现
匿名性	实现	实现	实现	实现	实现
抗合谋攻击					实现
抗重放攻击				实现	实现
计算总开销	高	高	高	低	低
安全性	低	低	低	低	高

从表 3 可以看出，改进方案与相关车载自组网方案对比，实现了 V_p 隐私、R_s 隐私、匿名性，具有抗合谋攻击和抗重放攻击的优点，且具有较高的安全性和效率.

6　结束语

车载自组织网的部署实施可以极大地提高人们的生活水平和生产力水平. 为促进车载自组织网络的发展应用，对宋成等[13]提出的车载网隐私保护方案进行了简要分析，发现该方案身份认证阶段存在漏洞，抵抗合谋攻击的证明中也存在安全漏洞. 在该方案的基础上，提出了一个增强安全性的，车载网隐私保护方案. 改进方案不仅可以保证发送者隐私、接收者隐私、匿名性，抵抗重放攻击，还可以抵抗合谋攻击. 安全分析结果表明，改进方案能满足更高的安全性需求，但在计算效率上，由于改进方案增加了几项操作，导致计算效率较文献[13]方案略有下降. 下一步的研究方向是在保证各方面安全性的前提下，进一步降低系统中各个部分的计算、通信等开销，提高系统的可靠性.

参考文献：

[1] Fiebig B. European traffic accidents and purposed solutions[C]//Proceeding of ITU-T Workshop on Standardisation in Telecommunication for Motor Vehicles. Geneva: [s. n.], 2003: 24-25.

[2] Mokbel M F. Privacy in location-based services: state-of-the-art and research directions[C]//8th International Conference on Mobile Data Management. Mannheim: IEEE, 2007: 228-228.

[3] Raya M, Hubaux J-P. Securing vehicular Ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

[4] Bellur B. Certificate assignment strategies for a pki-based security architecture in a vehicular network[C]//2008 IEEE Global Telecommunications Conference. New Orleans: IEEE, 2008: 1836-1841.

[5] Papadimitratos P, Calandriello G, Hubaux J-P, et al. Impact of vehicular communications security on transportation safety[C]//2008 IEEE INFOCOM Workshops. Phoenix: IEEE, 2008: 1-6.

[6] Sundari S, Ananthi M. Secure multi-party computation in differential private data with data integrity protection[C]// International Conference on Computing and Communications Technologies. Chennai: IEEE, 2015: 180-184.

[7] Lin X, Sun X, 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.

[8] Guo J, Baugh J P, Wang S. A group signature based secure and privacy-preserving vehicular communication framework[C]//2007 Mobile Networking for Vehicular Environments. Anchorage: IEEE Computer Society, 2007: 103-108.

[9] Sun X, Lin X, Ho P H. Secure vehicular communications based on group signature and ID-based signature scheme[C]//2007 IEEE International Conference on

Communications: Glasgow: IEEE, 2007: 1539-1545.

[10] Zeng S, Huang Y, Liu X. Privacy-preserving communication for VANETs with conditionally anonymous ring signature[J]. International Journal of Network Security, 2015, 17(2): 135-141.

[11] Shao J, Lin X, Lu R, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711-1720.

[12] 刘文, 罗守山, 杨义先, 等. 安全两方圆计算协议[J]. 北京邮电大学学报, 2009, 32(3): 32-35.
Liu Wen, Luo Shoushan, Yang Yixian, et al. A study of secure two-party circle computation problem[J]. Journal of Beijing University of Posts and Telecommunications, 2009, 32(3): 32-35.

[13] 宋成, 张明月, 彭维平, 等. 基于安全多方计算的车载网隐私保护机制[J]. 北京邮电大学学报, 2017, 40(3): 67-71.
Song Cheng, Zhang Mingyue, Peng Weiping, et al. Privacy protection mechanism based on secure multi-party computation in VANET[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(3): 67-71.

[14] Shi R H, Zhong H, Huang L S. A novel anonymous authentication scheme without cryptography[J]. Transactions on Emerging Telecommunications Technologies, 2014, 25(9): 875-880.

[15] Shi R H, Zhong H, Huang L S. A novel anonymous authentication scheme without cryptography[M]. John Wiley & Sons, Inc: [s. n.], 2014: 875-880.

[16] 赵圣楠, 蒋瀚, 魏晓超, 等. 一个单服务器辅助的高效 n 取 k 茫然传输协议[J]. 计算机研究与发展, 2017, 54(10): 2215-2223.
Zhao Shengnan, Jiang Han, Wei Xiaochao, et al. An efficient single server-aided k-out-of-n oblivious transfer protocol[J]. Journal of Computer Research and Development, 2017, 54(10): 2215-2223.

[17] 张福泰, 李继国, 王晓明. 密码学教程[M]. 武汉: 武汉大学出版社, 2006: 126.

[18] 蒋溢. 无线传感器网络路由安全关键技术研究[D]. 成都: 电子科技大学, 2015.