

基于同态加密和区块链技术的车联网隐私保护方案

王瑞锦^{1,2}, 唐榆程¹, 张巍琦¹, 张凤荔^{1,2}

(1. 电子科技大学信息与软件工程学院, 四川 成都 610054;

2. 网络与数据安全四川省重点实验室, 四川 成都 610054)

摘要: 为了解决传统车联网设备安全性相对较低可能威胁到用户隐私的问题, 提出了一种基于同态加密和区块链技术的车联网隐私保护方案。此方案将由二级节点组成的验证服务添加到所提模型中, 以实现模型中角色的权限控制。为了记录车联网设备信息, 设计基于同态加密(HEBDS)新的块数据结构, 使隐私数据可以经过 Paillier 加密算法处理后再写入区块, 并由获得记账权的网关节点写入区块链网络。该方案实现了数据在密文状态下的处理, 弥补了区块链网络中全部数据公开的不足。通过对该方案的安全性分析, 证明此方案具有不可伪造、隐私数据安全等特性。该方案通过对隐私数据的同态加密处理再上传区块链网络, 实现隐私数据以密文状态分发、共享和计算, 比传统车联网模型更能有效保护用户隐私。

关键词: 区块链; 同态加密; 车联网; 隐私保护

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020011

Privacy protection scheme for internet of vehicles based on homomorphic encryption and block chain technology

WANG Ruijin^{1,2}, TANG Yucheng¹, ZHANG Weiqi¹, ZHANG Fengli^{1,2}

1. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

2. Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China

Abstract: In order to solve the problem that the security of traditional internet of vehicles devices is relatively low, which may threaten the privacy of users, a privacy protection scheme based on homomorphic encryption and block-

收稿日期: 2019-11-20; 修回日期: 2020-01-17

通信作者: 王瑞锦, ruijinwang@uestc.edu.cn

基金项目: 国家自然科学基金资助项目(No.61802033, No.61472064, No.61602096); 四川省科技计划基金资助项目(No.2018GZ0087, No.2019YJ0543); 博士后基金资助项目(No.2018M643453); 广东省国家重点实验室基金资助项目(No.2017B030314131); 网络与数据安全四川省重点实验室开放课题基金资助项目(No.NDSMS201606)

Foundation Items: The National Natural Science Foundation of China (No.61802033, No.61472064, No.61602096), Sichuan Science and Technology Plan (No.2018GZ0087, No.2019YJ0543), Chinese Postdoctoral Science Foundation (No.2018M643453), Guangdong Provincial Key Laboratory Project (No.2017B030314131), Network and Data Security Key Laboratory of Sichuan Province Open Issue (No.NDSMS201606)

论文引用格式: 王瑞锦, 唐榆程, 张巍琦, 等. 基于同态加密和区块链技术的车联网隐私保护方案[J]. 网络与信息安全学报, 2020, 6(1): 46-53.

WANG R J, TANG Y C, ZHANG W Q, et al. Privacy protection scheme for internet of vehicles based on homomorphic encryption and block chain technology[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 46-53.

chain technology was proposed. This scheme added the authentication service composed of two level nodes to the proposed model to realize the permission control of roles in the model. In order to record the information of the internet of vehicles devices, a new block data structure based on homomorphic encryption (HEBDS) was proposed, which enabled the privacy data to be written into the block after being processed by the Paillier encryption algorithm, and then written into the blockchain network by the gateway node obtaining the accounting right. This scheme realized the data processing in ciphertext state, and made up for the shortage of all data disclosure in blockchain network. Through the analysis of the security of the scheme, it is proved that the scheme has the characteristics of unforgeability and privacy data security. Through homomorphic encryption of privacy data and upload to blockchain network, the scheme can distribute, share and calculate privacy data in ciphertext state, which can protect customer privacy more effectively than traditional internet of vehicles model.

Key words: blockchain, homomorphic encryption, internet of vehicle, privacy protection

1 引言

随着城市智慧化的加速发展,车联网为人类提供了交通管理和出行等方面的便利,也成为智慧城市的重要标志,已被写入国家“十三五”规划中^[1]。同时,越来越多人员、车辆的参与和高度动态的拓扑结构,导致车联网中个人信息可用性和用户隐私保护重要性之间不协调的矛盾,车辆人员信息或车辆位置信息泄露等安全风险对车联网的广泛应用形成了桎梏。

以智慧城市车联网中的停车收费服务为例,当用户注册、停车付费等操作给服务提供商后,用户的很多隐私信息(如爱好、车辆信息、位置、习惯等)都会被服务提供商得到,这个过程中如何做好用户的隐私保护成为关键^[2-3]。因此,车联网在提供服务的同时需要重点设计隐私保护模型,使用户既能享有高质量的服务,又能避免自己的隐私信息被第三方非法获取^[4]。

区块链技术中的去中心化、匿名化特性为解决车联网中相关的问题提供了思路。但随着区块链平台的大量涌现,智能合约功能逐渐丰富,用户的数量也在不断增加,区块链需要存储和传输的数据越来越多,由于大部分区块链平台上的数据都是对全网公开的,缺乏有效的隐私保护方案。因此,在基于公有链或者联盟链的车联网设计中,如何利用加密处理来保护车辆和人员信息的隐私性成为探讨的话题。

同态加密技术作为一种特殊的加密方案,它允许在不知道私钥的情况下对加密数据执行特定的计算,使计算之后得到的加密数据解密后的结

果与对明文执行相同的计算得到的结果相同^[5-6]。利用同态加密技术解决车联网区块链上互不信任的参与方之间进行互操作的信息安全问题,即同态加密技术将车联网区块链中发布的数据内容和交互数据、数据状态属性等进行加密,从而在保证数据安全的同时完成对数据的操作,使车联网用户的隐私数据得到有效保护。

2 相关工作

车联网体系源自物联网,是由车载信息单元、路边单元以及信息管理平台构成的智慧交通网络^[7]。车联网系统的普及需要打消使用者对其隐私信息暴露的顾虑,对车辆隐私信息做到有条件的保护,即正常情况下对车辆的位置信息、驾驶信息、路线信息、驾驶员身份信息、相关交易信息的保密,同时在出现非正常情况(如肇事逃逸)下,特权人员(警察)可以揭发消息发送者的相关信息^[8]。传统的车联网分为应用层、网络层和感知层^[9]。感知层通过传感器和GPS定位技术,实时感知车辆的位置信息和车辆的状态信息^[10];网络层把感知层获取的信息通过协议传递到应用层;应用层与用户信息进行交互。虽然现有的车联网可以通过某种方式保护用户的隐私,但信息安全仍然存在一些潜在的风险。用户的隐私或敏感数据被某个车联网平台或机构集中存储和处理,如果集中式数据库受到攻击并且数据泄露,无法保证交易数据隐私性和安全性^[11]。

区块链是一个分布式、不可篡改、公开的分布式数据库,它为车联网的安全性和隐私保护提供了新的途径^[12-13]。区块链技术作为一种集加解

密技术、数字签名技术、密钥分存技术、分布式存储技术及一致性问题与共识算法于一身的复合技术,在数字资产交易、食品溯源、证据存证,电子发票、版权认证等领域中找到了新颖的应用。根据区块链的特征,它将各个数据块进行链接,在每个区块中,都存在两个结构——区块头和区块体^[14-15]。区块头包含了版本号、目标散列值、前一个区块地址、时间戳等信息。而区块体中封装了当前所有交易的数据结构。这种数据结构能够从预先选择的节点跟踪每个块的信息并且影响后续节点的信息。其加密方法确保恶意攻击难以篡改信息。根据区块链的可追溯性,车联网用户可以查看所有的交易记录,同时区块链的匿名性保证了人们无法匹配其他人的账户。区块链信息的高度透明、防篡改,可有效降低隐私泄露的风险。

针对基于区块链技术在车联网隐私保护和数据安全上的应用,Arora 等^[16]提出了一种在车联网中提供车辆节点之间认证和安全数据传输的方法,以确保节点之间准确的信息通信;Knirsch 等^[17]基于区块链技术提出了一种在不公开电动车辆位置信息的基础上匹配车辆附近性价比最高的充电站的方法;Jeong 等^[18]设计了一种基于区块链的电动汽车充电站计费系统,可以使电动汽车和充电站在相互认证之后将计费信息存储在区块链中并防止修改;Li 等^[19]提出了一种基于新兴区块链范式的新型分散安全设计架构,用于保护基于车联网的交通信号控制系统免受恶意数据攻击。总结上述文献,结合区块链和物联网技术,可以解决物联网隐私安全和隐私保护的相关问题。区块链的匿名性也使其他用户无法匹配其他人的账户。但是,针对车联网这一特定领域的实际用途,完全匿名与特权人员对信息的揭发这一需求相违背。本文提出一种方法,结合区块链和同态加密的技术特性,将车联网的相关数据分为隐私数据和普通数据,使隐私数据的处理始终在密文状态,保证仅有相关人员能读取相关信息。

3 基于同态加密的块数据结构

与通常的区块链结构不同,为了使敏感数据得到保护,本文提出一种基于同态加密的新的块数据结构。

本文将收集的车联网节点数据 msg 分为公共数据 (msgPD) 和敏感数据 (msgSD), $\text{msg} = \text{msgPD} \cup \text{msgSD}$, 对于 msgSD 需要进行同态加密。这里,选用有加法同态性质的 Paillier 加密算法,其步骤如下。

1) 生成密钥

随机选取两个大质数 p, q , 令 $N = p \cdot q$, λ 是 $p-1$ 和 $q-1$ 的最小公倍数,再随机选取一个整数 $g \in Z_{N^2}^*$ (小于 N^2 并与 N^2 互质的整数), g 满足 $\gcd(L(g^{\lambda} \bmod N^2), N) = 1$, 则 (N, g) 和 λ 分别表示公钥和私钥。

注: $L(x) = (x-1)/N$, $\gcd(x, y)$ 表示计算 x, y 的最大公约数。

2) 加密

随机选择一个整数 $r \in Z_{N^2}^*$, 对于敏感数据 $\text{msgSD} \in Z_N$, 利用公钥 (N, g) 加密后得到相应密文 $c = E(\text{msgSD}, r) = (g^{\text{msgSD}} \cdot r^N) \bmod N$ 。

3) 生成区块散列

$\text{msg} = c \cup \text{PD}$ (敏感数据 c , 非敏感数据 PD), 再使用区块链分配的私钥对 msg 签名, 并对签名后的不能抵赖的数据通过散列生成唯一散列值, 并写入车联网区块链的区块头中。

根据 Paillier 加密算法的加法同态性质, 某车辆两次停车消费, 记 m_1, m_2 是两次停车的费用, $m_1, m_2 \in Z_N^*$, 任取 $r_1, r_2 \in Z_{N^2}^*$, 加密可得

$$\begin{aligned} c_1 &= E(m_1, r_1), c_2 = E(m_2, r_2) \\ c_1 \cdot c_2 &= E(m_1, r_1) \cdot E(m_2, r_2) = \\ &= (g^{m_1+m_2} \cdot (r_1 \cdot r_2)^N) \bmod N \end{aligned}$$

满足 $F(E(x), E(y)) = E(x+y)$, F 代表任意运算。即可以在不公布两次停车费用的前提下得到停车费用和的密文。

4) 解密

若需要得到明文 msg, 则需要对密文 c 利用私钥 λ 解密。

$$\text{msg} = D(c) = [L(c^{\lambda} \bmod N^2) / L(g^{\lambda} \bmod N^2)] \bmod N$$

针对求和后的数据解密如下。

$$\begin{aligned} D(c_1 \cdot c_2) &= D[E(m_1, r_1) \cdot E(m_2, r_2)] = \\ &= D[(g^{m_1+m_2} \cdot (r_1 \cdot r_2)^N) \bmod N] = (m_1 + m_2) \bmod N \end{aligned}$$

图 1 是按照同态加密得到的新的区块链节点后的数据结构。

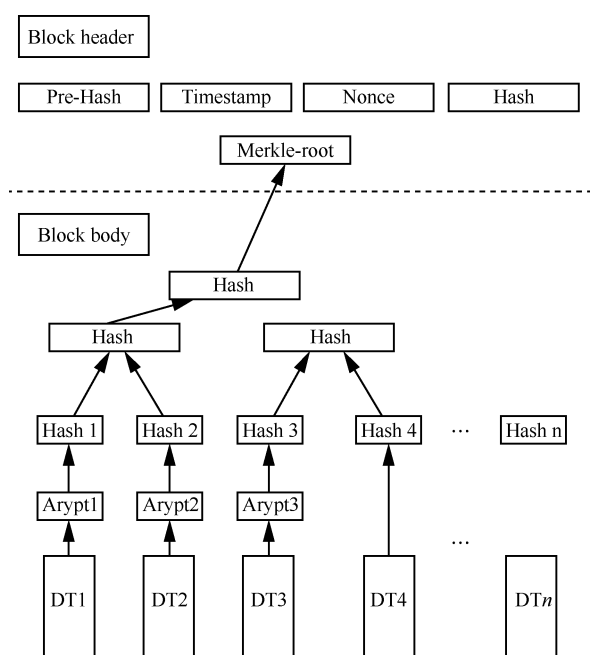


图 1 基于同态加密的块数据结构

Figure 1 Block data structure based on homomorphic encryption

如图 1 所示，该结构数据不直接散列数据 DT，而是将数据划分为公开数据和隐私数据，针对隐私数据，先同态加密再散列。

3 隐私保护模型

本节主要介绍基于区块链和同态加密技术的车联网隐私保护方案的模型。

3.1 模型架构

从车联网隐私保护模型设计的角度来看，服务于此模型的区块链网络从下至上可以抽象为 4 个实现层面，分别是数据与网络组织协议、分布式共识协议、基于分布式虚拟机的自组织框架和人机交互层面，如图 2 所示。

3.2 节点构成

与传统的车联网不同，为了更好地管理其成员并加密其中相关的敏感数据，如图 3 所示，本文考虑设置 3 类节点，即车联网的网关节点 G_i 、车联网的传感器节点 S_i 和车联网的二级节点 P_i 。

在这个过程中，由 P_i 生成节点密钥和同态加密密钥，并且把密钥分发给与之相连的所有 G_i 。同时， S_i 将实时收集相关数据，并将集成数据上传给网关节点 G_i ， G_i 收集 S_i 在传输范围内的所有数据，通过细粒度的划分，把数据区划分为普

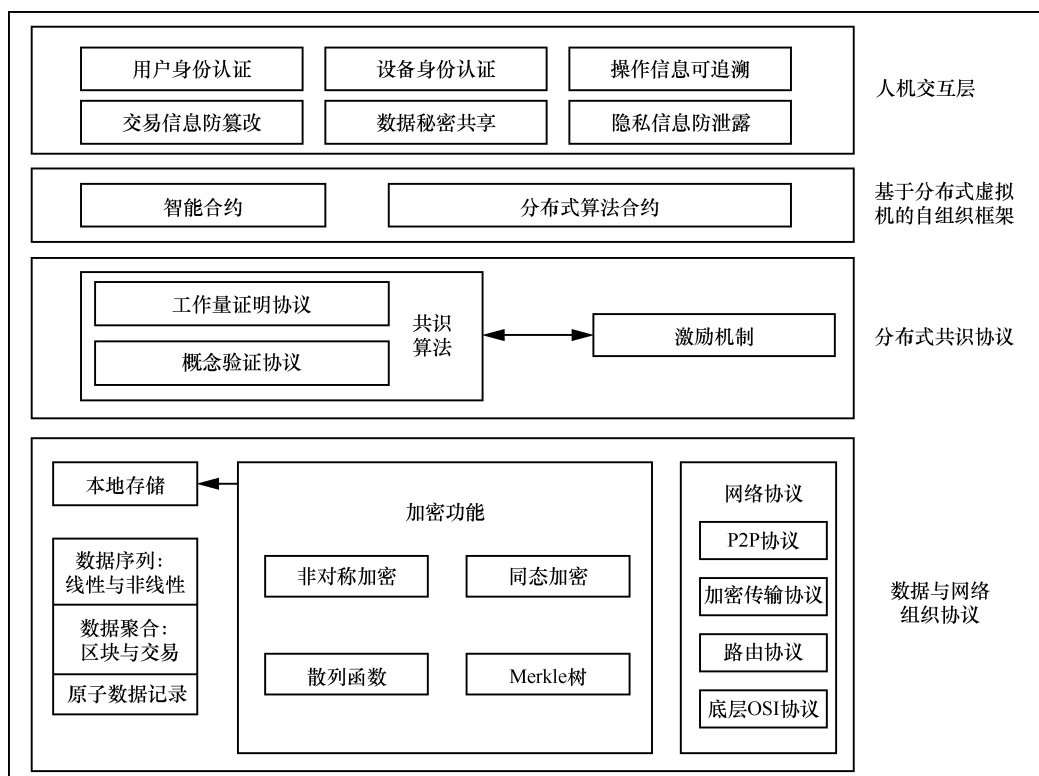


图 2 模型架构

Figure 2 Model architecture

通数据和隐私数据,对需要保护的隐私信息采用同态加密算法进行加密,从而保护车联网用户的隐私敏感数据。

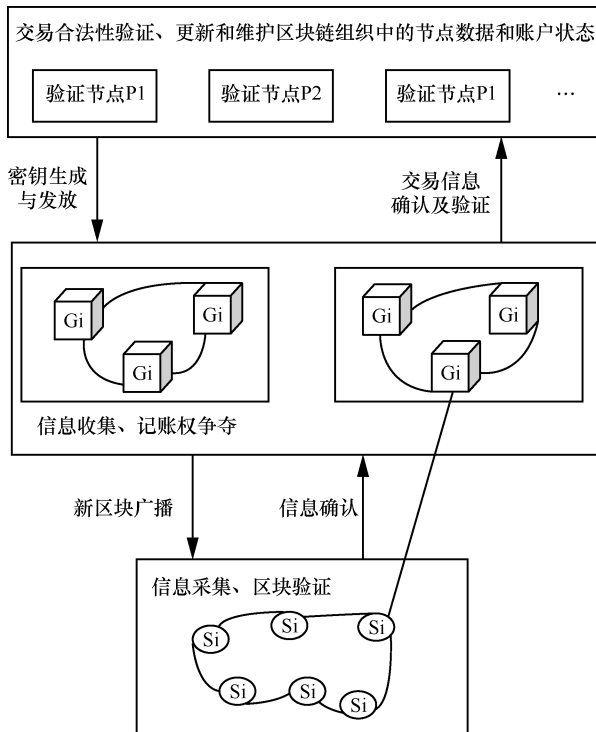


图3 节点构成
Figure 3 Node composition

P_i 作为二级节点,所有的 P_i 构成证书服务的成员,主要负责整个网络中证书的管理并向区块链网络中的成员提供基于数字证书的身份信息,同时可以生成或取消成员的身份证书。增加 P_i 服务可以按照不同身份进行权限管控,主要处理智能合约,检查车联网的交易数据的合法性,以及更新和维护区块链组织中车联网的节点数据和账户状态。

G_i 作为网关节点,主要收集 S_i 采集到的相关车联网数据,并使用 P_i 分发的密钥对车联网隐私数据进行同态加密,这个过程中通过设计工作量证明 (POW) 算法,获得记账权。成功的节点可以打包新的区块,新区块在所有节点中进行广播,通过工作量证明算法和竞争机制完成合法性验证后,此次发起的交易数据才能真正地被写入区块链网络。

S_i 作为传感器节点,收集相关信息,传输给 G_i ,并由 G_i 处理后写入车联网的区块链网络。

3.3 模型工作过程

隐私保护模型工作的具体过程如下。

1) 形成车联网区块链的主链并生成首区块

按照 POW 规则,不断在车联网的 G_i 中选择记账节点,及有获得记账权的车联网节点,将交易打包形成区块,在获得大多数其他车联网节点验证同意后加入区块链。

2) 分配节点密钥和同态加密密钥

首先,车联网节点公钥和同态加密公钥由 P_i 生成,同时把节点私钥和同态加密私钥通过秘密信道分配给每一个 G_i 。同时,相应的记账车联网节点应该记录块中的同态公钥。

3) 发布已经签名的数据包

当车联网的网关节点收集到传感器节点 S_i 发送的信息 msg 时,首先把 msg 分为敏感数据 ($msgSD$) 和公开数据 ($msgPD$),同时采用同态加密把 $msgSD$ 加密 (如 Paillier),把同态加密后的车联网数据和 $msgPD$ 打包进数据包 (DP),再把 DP 用网关节点私钥进行签名。最后,DP 被 G_i 同步到车联网的区块链网络。

4) 生成块

根据工作量证明算法,在 G_i 中选择记账节点,簿记节点将一段时间内的所有信息以 Merkle 树的形式写入块头,并存储 ParentHash、Coinbase、TimeStamp、Merkle 树,块体中的 root、Number、Nonce 和其他参数。最后,它们将块头和块体打包成一个新的块,该块在主链的末尾链接。按照时间戳的顺序把这些正确的块链接起来形成链数据结构,最终构建车联网区块链。

3.4 模型仿真实验

在通常的车联网中,汽车所产生的数据往往是中心化存储且是弱匿名性的,数据的处理过程和存储存在数据泄露的风险,为解决这一问题,本文构建了基于区块链和同态加密技术的车联网隐私保护模型,并对其进行了仿真实验。笔者成功搭建了基于工作量证明算法 (挖矿难度系数可变) 的区块链网络,添加了相应的节点。

仿真实验如下:在某一区域有若干个车联网网关节点,由于模拟实验环境中计算量有限,随机选择了车联网的 50 个网关节点 G_i 进行仿真实验。将每辆车传感器节点的状态数据上传至网关

节点 G_i 。在实验中,假设每个节点收集3种隐私数据:车联的行驶里程数、车辆的停车缴费金额和燃油流量信息。每个 G_i 收集的用户隐私数据的明文如表1所示。

表1 G_i 收集的用户隐私数据的明文数据
Table 1 G_i clear text data of collected user privacy data

网关节点	行驶里程/公里	停车缴费金额/元	燃油流量/升
G_{i_1}	600	150	70
G_{i_2}	800	220	80
G_{i_3}	1 000	310	90
$\vdots$	$\vdots$	$\vdots$	$\vdots$
G_{i_50}	2 000	840	130

由 G_i 所处理后的数据被加密成表2的形式。

假设停车场收费方需要判断 G_{i_1} 是否有足额费用以支付停车费用,它仅需要在区块链网络中读取消费金额的加密数据,并在密文的状态下比较余额和消费金额的大小以判断此次交易是否成功,这就把司机个人信息与此次交易信息完全隔离开,保证了隐私信息的安全。

4 攻击模型和性能实验分析

4.1 攻击模型

针对此方案中可能出现的不安全节点对整个模型的影响,以及为了对存储在其中的车联网隐私数据的安全保障,笔者分析了几种攻击案例。

1) 假设某个二级节点 P_{i1} 被攻击为不安全节点,以下数据将被泄露。

① 分配的同态加密的公钥和私钥。

② G_i 请求的经过身份验证的同态加密数据。

③ 对应 G_i 上的数据也可以被解密和获取,但这些数据都是同态加密的数据,这样敏感数据不会泄露。

④ 过去这段时间内存储在区块链上的由 P_{i1} 分配的同态加密密钥加密和签名的数据。

由于 P_{i1} 无法发起查询区块链中先前数据块内容的请求,在这种情况下,攻击对此模型中受保护的敏感车联网节点数据没有影响。

2) 假设某个网关节点 G_{i_1} 被攻击为不安全节点,以下数据将被泄露。

① 收集的车联网传感器的信息,即一段时间内数据区块中的信息。

② 先前区块的信息。由于先前区块记录的是加密的车联网节点敏感数据,其不能被解密,在这种情况下,攻击对此模型中受保护的敏感车联网数据没有影响。

③ 由 P_{i2} 分配的公钥和私钥。

④ 所有通过此节点进行同态加密的车联网隐私数据。

在所有交易数据都是密文的状态下,攻击对模型中受保护的敏感车联网数据没有影响。

3) 假设多个网关节点 G_i 被攻击,创建一个新的区块链分支。

p =未被攻击节点在一轮竞争中领先的概率

q =已被攻击节点在一轮竞争中领先的概率

q_z =已被攻击节点在落后未被攻击节点 z 个

区块最终追上未被攻击节点的概率如式(1)所示。

表2 G_i 所处理后的数据被加密数据
Table 2 G_i the processed data is encrypted data

网关节点	行驶里程/公里	停车缴费金额/元	燃油流量/升
G_{i_1}	7263129731273912637021381237980207 9812630283791232198362170692092713 92136270361237632106217931	2653783173189267636734906726351038 1003762731239389403189239230189187 19301803178210319392837131	2653783173189267636734906726351038 1003762731239389403189239230189187 19301803178210319392837131
G_{i_2}	8731293710203964005487379812791078 1264981798126498174981708916238012 73891273981641647189130065	8398837810007382662918173219882738 7913077887783278738748710001237271 02739973287031023702378101	3092329040321390324128448717237130 3110219331378454536161819773281918 02103131737137813783912033
G_{i_3}	2721637812631961400912892100392817 2174672391294984017017037219831283 12312312312309	2093082310989312928312981098219832 1378211816166513727232789182388781 20012710231636	5256351820203782837118382272647197 8316191072137817200073818327182301 82181021811882
$\vdots$	$\vdots$	$\vdots$	$\vdots$
G_{i_50}	4090803291789217481671389182361923 7897412767127938763913891298382198 12941987972082	7398162736178713100192893213912823 7732728378746801012721029830210983 92893102018391	7610081023912376345546814183717300 3171873812637163714732378459589319 31621772900621

$$q_z = \begin{cases} 1, & q \leq p \\ \left(\frac{q}{p}\right)^z, & p > q \end{cases} \quad (1)$$

当 $p > q$ 时, 随着车联网区块数的增长, 攻击成功的概率呈指数下降趋势。假设诚实节点领先 z 个区块, 且它们耗费平均预期时间才产生一个区块, 那么攻击者的潜在趋势是一个泊松分布, 期望值为

$$\lambda = z \frac{q}{p} \quad (2)$$

为了计算攻击者追赶上的概率, 本文将攻击者取得进展区块数量的泊松分布的概率密度, 乘以在该数量下攻击者依然能够追赶上的概率。计算如式(3)所示。

$$\sum_{k=0}^{+\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{(z-k)}, & k \leq z \\ 1, & k > z \end{cases} \quad (3)$$

避免对无限数列求和, 可以将其化为下面的形式。

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \quad (4)$$

对分叉攻击成功的概率进行模拟, 模拟结果如表3所示。可以看到, 创建一条链的成功率随着 z 的增加而呈指数级下降, 除非攻击者掌握的算力接近全网算力的50%, 否则从概率上来说几乎是不可能成功的。

表3 模拟结果
Table 3 Simulation results

z	$q=0.1$	$q=0.3$
$z=1$	0.20458727394278242	0.627749109982254
$z=2$	0.05097789283933862	0.4457170995239838
$z=3$	0.013172241678896482	0.3245841018204811
$z=4$	0.0034552434664851736	0.2391268577972393
$z=5$	0.0009136821879279122	0.1773523113609451
$z=10$	0.0000012612862196786	0.04166047996897915

4.2 性能分析

1) 数据有效性

本文所采取的是基于同态加密的数据结构。

由于区块链技术本身具有防篡改、公开透明的特性, 每个 G_i 可以通过在块形成后同步区块链块得到永久的数据库。其中, 公开数据可以直接从数据块获得并计算。隐私数据也可以在不公开隐私数据的前提下利用 Paillier 的加法同态性质进行计算, 并在获得授权后可以查看相应的结果。

2) 数据隐私性

本文将收集的数据进行区分, 隐私数据经过同态加密后, 共享、复制、分发和计算使用都是以密文的状态, 不会造成隐私信息的泄露。

3) 系统稳健性

本文方法是在车联网区块链网络上进行构建, 满足可用性 (Availability)。同时, 基于车联网区块链网络的链式结构和分布式存储规则, 在非篡改的前提下, 每个 G_i 都能参与系统的计算和验证成果, 这不仅提高了系统的计算能力, 还增强了系统的稳健性。

5 结束语

本文基于同态加密技术, 在区块链共享透明的环境下能确保车联网用户数据的隐私。通过设计车联网区块链的块数据结构、网络构建、节点之间协同工作等机制, 保证了车联网用户的隐私信息, 并通过攻击模型和性能分析证明了安全性和可用性。如何在保证车联网隐私数据安全的前提下, 采用激励措施等提高效率是下一步研究的主要工作。

参考文献:

- [1] DENNIS R, OWENSON G, AZIZ B. A temporal blockchain: a formal analysis[C]//2016 International Conference on Collaboration Technologies and Systems (CTS). 2016: 430-437.
- [2] DIMITROV D V. Medical Internet of things and big data in healthcare[J]. Healthc Inform Res, 2016, 22(3): 156-163.
- [3] SHEELA M A, VIJAYALAKSHMI K. A novel privacy preserving decision tree induction[C]//IEEE on Information & Communication Technologies (ICT). 2013, 1075-1079.
- [4] LAKSHMI M N, RANI K S. SVD based data transformation methods for privacy preserving clustering[J]. International Journal of Computer Applications, 2013, 78(3): 39-43.
- [5] BONAM J, REDDY A R, G. Kalyani. Privacy preserving in association rule mining by data distortion using PSO[C]//ICT Critical Infrastruct, 48th Annu Conv Comput. 2014, 551-558.
- [6] 房卫东, 张武雄, 单联海, 等. 无线传感器网络用户认证协议研究进展[J]. 网络与信息安全学报, 2017, 3(1): 1-12.

- FANG W D, ZHANG W X, SHAN L H, et al. Research progress on user authentication protocol for wireless sensor networks [J]. Chinese Journal of Network and Information Security, 2017, 3(1): 1-12.
- [7] 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]. 信息安全, 2018(8): 64-72.
- MA R, CHEN X, LIU H, et al. Research about user privacy measurement and privacy protection in mobile crowd sensing[J]. Information Network Security, 2018(8): 64-72.
- [8] KIYOMOTO S, RAHMAN M S, BASU A. On blockchain-based anonymized dataset distribution platform[C]//IEEE International Conference on Software Engineering Research, Management and Applications. 2017:85-92
- [9] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]// IEEE Symposium on Security & Privacy. 2014: 459-474.
- [10] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151:1-32
- [11] PETERS G W, PANAYI E. Understanding modern banking ledgers through Blockchain technologies: future of transaction processing and smart contracts on the internet of money[M]//Banking Beyond Banks and Money. 2016: 239-278.
- [12] DHILLON V, METCALF D, HOOPER M. The hyperledger project[M]//Blockchain Enabled Applications. 2017: 139-149.
- [13] ZHANG Y H, HU Y, XIE J, et al. Efficient ring signature schemes over NTRU lattices[J]. Security & Communication Networks, 2016.
- [14] WU L, MENG K, XU S, et al. Democratic centralism: a hybrid blockchain architecture and its applications in energy internet[C]//IEEE International Conference on Energy Internet (ICEI). 2017: 176-181.
- [15] LIND J, NAOR O, EYAL I, et al. Teechain: reducing storage costs on the blockchain with offline payment channels[C]//The 11th ACM International Systems and Storage Conference. 2018: 125-125.
- [16] ARORA A, YADAV S K. Block chain based security mechanism for Internet of vehicles (IOV)[C]//The 3rd International Conference Internet Things and Connected Technologies (ICIOTCT). 2018.
- [17] KNIRSCH F, UNTERWEGER A, ENGEL D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions[J]. Computer Science Research Development, 2018, 33(1): 71-79.
- [18] JEONG S, DAO N N, LEE Y, et al. Blockchain based billing system for electric vehicle and charging station[C]//The Tenth International Conference on Ubiquitous and Future Networks (ICUFN). 2018.
- [19] XU C, WANG K, XU G, et al. Making big data open in collaborative edges: a blockchain-based framework with reduced resource requirements[C]//IEEE International Conference on Communications (ICC). 2018: 1-6.

[作者简介]



王瑞锦（1980—），男，甘肃天水人，博士，电子科技大学副教授，主要研究方向为信息安全、隐私保护和区块链。



唐榆程（1996—），男，四川南充人，电子科技大学硕士生，主要研究方向为区块链和隐私保护。



张巍琦（1995—），男，陕西宝鸡人，电子科技大学硕士生，主要研究方向为知识图谱、数据挖掘和数据可视化。



张凤荔（1963—），女，河南郑州人，博士，电子科技大学教授、博士生导师，主要研究方向为大数据安全、隐私保护和区块链。