基于Tangle网络的移动群智感知数据安全交付模型

赵国生[①] 张 慧*[①] 王 健[②]

[①](哈尔滨师范大学计算机科学与信息工程学院 哈尔滨 150025)

[②](哈尔滨理工大学计算机科学与技术学院 哈尔滨 150080)

摘 要：针对现有群智感知平台在数据和酬金交付过程中存在的安全风险和隐私泄露问题，该文提出一种基于Tangle网络的分布式群智感知数据安全交付模型。首先，在数据感知阶段，调用局部异常因子检测算法剔除异常数据，聚类获取感知数据并确定可信参与者节点。然后，在交易写入阶段，使用马尔科夫蒙特卡洛算法选择交易并验证其合法性，通过注册认证中心登记完成匿名身份数据上传，并将交易同步写入分布式账本。最后，结合Tangle网络的累计权重共识机制，当交易安全性达到阈值时，任务发布者可进行数据和酬金的安全交付。仿真试验表明，在模型保护用户隐私的同时，增强了数据和酬金的安全交付能力，相比现有感知平台降低了时间复杂度和任务发布成本。

关键词：移动群智感知；Tangle网络；感知数据；安全交付

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2020)04-0965-07

DOI: 10.11999/JEIT190370

A Mobile Crowdsensing Data Security Delivery Model Based on Tangle Network

ZHAO Guosheng[①] ZHANG Hui[①] WANG Jian[②]

[①](*College of Computer Science and Information Engineering*, *Harbin Normal University*, *Harbin* 150025, *China*)

[②](*School of Computer Science and Technology*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

Abstract: Considering the security risks and privacy leaks in the process of data and reward in the Mobile CrowdSensing (MCS), a distributed security delivery model based on Tangle network is proposed. Firstly, in the data perception stage, the local outlier factor detection algorithm is used to eliminate the anomaly data, cluster the perception data and determine the trusted participant. Then, in the transaction writing stage, Markov Monte Carlo algorithm is used to select the transaction and verify its legitimacy. The anonymous identity data is uploaded by registering with the authentication center, and the transaction is synchronously written to the distributed account book. Finally, combined with Tangle network cumulative weight consensus mechanism, when the security of transaction reaches its threshold, task publishers can safely deliver data and rewards. The simulation results show that the model not only protects user privacy, but also enhances the ability of secure delivery of data and reward. Compared with the existing sensing platform, the model reduces the time complexity and task publishing cost.

Key words: Mobile CrowdSensing (MCS); Tangle network; Perceived data; Secure delivery

收稿日期：2019-05-23；改回日期：2019-09-03；网络出版：2019-09-17

*通信作者： 张慧 18746424159@163.com

基金项目：国家自然科学基金(61202458, 61403109)，黑龙江自然科学基金(F2017021)，哈尔滨市科技创新人才研究专项资金(2016RAQXJ036)

Foundation Items: The National Natural Science Foundation of China (61202458, 61403109), The Natural Science Foundation of Heilongjiang Province (F2017021), The Harbin Science and Technology Innovation Research Funds (2016RAQXJ036)

1 引言

移动群智感知(Mobile CrowdSensing, MCS)是将人与设备有机组合为大量类似具备传感器模块的设备节点，通过物联网或互联网将收集到的信息进行共享和计算的一种方式。群智感知的运行依赖于大量用户的参与。然而，人本身具有自私性，可能会发起欺骗或共谋共计以最大化自身利益，因此，设计一种安全可信的感知数据交付模型尤为必要[1–3]。

目前，移动群智感知系统的运行大多基于中心化模型，其面临的安全威胁主要包含两个方面。第一，用户身份隐私泄露问题。Huang等人[4]利用K匿名算法结合区域中心坐标并基于微聚合(micro-aggregation)设计了一种隐私保护方案。Dong等人[5]考虑第三方服务器不可信，使用属性加密方式保护用户位置信息。Christin等人[6]设计了一种结合假名并去中心化的隐私保护机制。文献[7]利用参与者之间存在的合作机制，设计了一种无需依赖中心服务器的隐私保护机制PriSense，最大限度的保护用户隐私。第二，恶意攻击行为对数据隐私的威胁，如错误数据攻击、返回攻击、共谋攻击、女巫攻击等。为此，Christin等人[8]设计了名为IncogniSense的声望框架，防止参与者信息被恶意节点盗取、非法牟利。Restuccia等人[9]试图借助移动安全代理来保障信息质量，抵抗共谋攻击及错误数据攻击。Chang等人[10]利用群智感知中的云层信任管理机制，提出一种女巫攻击检测方法。

随着中心化群智感知系统的安全问题愈发严重，研究人员现如今尝试利用分布式系统来解决这些问题。Li等人[11]提出一种分散式众包系统框架CrowdBC，利用区块链去中心化的特点，解决了中心化模型服务器易遭受单点故障、分布式拒绝服务攻击(Distributed Denial of Service, DDoS)及女巫攻击等问题，但此框架并未充分考虑区块链透明性与数据保密之间存在的矛盾关系。此时，Lu等人[12]针对该问题设计了一种匿名机制，防止恶意参与者利用匿名机制实现双花，但该机制未考虑恶意攻击者上传病毒后对系统整体造成的损害。

针对上述问题，本文设计了可匿名的Tangle分布式群智感知数据交付模型。主要贡献如下：

(1) 基于区块链对数据去中心化存储的特性，避免第三方介入带来的安全问题；

(2) 数据的发布与交易验证都由参与者节点完成，不存在挖矿过程，降低任务发布成本；

(3) 由认证注册中心登记，完成身份匿名数据上传，防止服务器隐私泄露；

(4) 基于Tangle结构的安全性，保证数据安全和用户工作的完整性和保密性。

2 基于Tangle网络的群智感知模型

参与者作为节点完成数据采集、交易验证及数据发布。一个交易的成功验证间接证明以往交易的安全性，Tangle网络随着交易的增加越来越安全。酬金支付过程由嵌入在Tangle网络中的智能合约自动完成。节点采集数据耗费一定量资源，只要证明其数据可用，则证明节点做了一定量工作，将此过程代替工作量证明(Proof of Work, PoW)，解决了传统链式账本的算力浪费问题。

2.1 模型结构

基于Tangle网络的感知数据交付模型由以下3部分组成，角色阐述如下：

(1) 任务发布者(task publisher)：将任务提交至平台并愿意为获得感知数据支付相应酬金的组织或者个人；

(2) 参与者(participant)：使用移动感知设备，按照任务需求进行数据采集的人员；

(3) 平台基础设施(platform infrastructure)：由任务服务器(Task Server, TS)、Tangle网络和支付服务器(Payment Server, PS)组成。数据交付模型如图1所示。

首先，TS 发布来自任务发布者的感知任务(①)，参与者定期访问TS，搜索是否有适合自身的任务并选择性地下载(②)；然后，参与者按照任务属性等信息，利用感知设备采集数据(③)并上传到TS(④)。在该过程中，参与者可向认证注册中心(Registration Authority, RA)申请匿名身份。接着， TS调用局部异常因子(Local Outlier Factor, LOF)检测算法选出一个获胜节点(winner)。该节点需在Tangle网络中验证另外两笔交易的合法性，随后将该笔交易同步写入分布式账本(⑤)。PS可定时查询Tangle中某笔交易的权重(⑥)，当权重达到一定阈值，PS可将酬金支付给该获胜节点(⑦)。

2.2 数据感知

假设多个任务发布者$R=\{R_1,R_2,\cdots,R_n\}$在云端平台发布了n个不同的感知任务，参与者

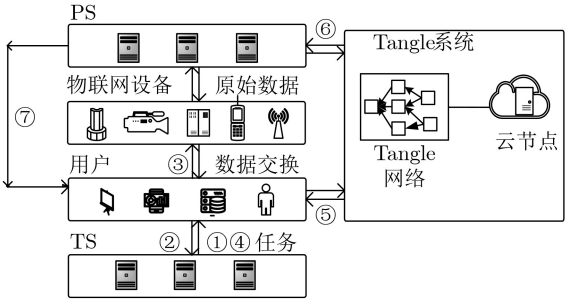

图 1 基于Tangle网络的感知数据交付模型

$N=\{N_1,N_2,\cdots,N_n\}$负责接收和竞争任务。本文将平台和任务发布者进行绑定，对于参与者而言，平台即任务发布者。

(1) 任务分发

任务发布者$R=\{R_1,R_2,\cdots,R_n\}$向平台提交任务请求，TS将当前收到的任务根据节点的位置信息D，将同一份数据采集任务分发给k个邻近的节点，此时同一任务将由k个节点共同完成，并定义该任务的感知数据为$T=\{T_1,T_2,\cdots,T_k\}$。

(2) 选择获胜节点

节点N_i用自己的私钥$\mathrm{sk_i}$对采集到的数据T_j签名，执行该任务的所有节点$N_i(0<i\le k)$将数据上传至TS，以位置作为决策指标调用LOF算法(见表1)对数据进行分析[13]，剔除异常数据，得到一个可靠数据集的聚类$Tj_i(0<j\le k)$，服务器从Tj_i中随机的选取一份数据(transaction)成为可用数据，并根据任务的大小为其设置一个时间参数，获胜节点Nj_i将有权将数据交易写入Tangle网络。如果Nj_i在T时间内未发布该任务的感知数据，服务器将从Nj_i中重新选择另一个Nj_k，使其最终能够完成数据的发布。

3　数据交付

Tangle网络需要创始块在初始为一部分的支持者分发一定的IoTA代币，奖励给加入模型中的节点。交易的连接结构如图2所示。

其中Tangle网络定义如下：

定义1 Site 存储交易，每条有向边为一个交易的验证过程，分为直接验证和间接验证。

定义2 权重 每个Site都被绑定了一个权重，其中权重被定义为一个3进制的变量。

表 1　算法1：基于参与者选择的LOF算法

输入：参与者的位置信息集N, k近邻参数

输出：前k个数据的LOF

(1) 计算任意数据点之间的欧式距离$\mathrm{disk}(i,j)$;

(2) 计算所有数据点和其前k个数据点间的距离$\mathrm{disk}_k(i)$;

(3) 计算所有数据点的k距离邻居$N_K(i)$; $N_K(i)=\{i'\mid i'\in N,\ \mathrm{dist}(i,i')\le \mathrm{dist}_k(i)\}$

(4) 计算所有数据点的局部可达密度$\mathrm{lrd}_k(i)$:

$$\mathrm{lrd}_k(i)=\frac{\|N_K(i)\|}{\sum\limits_{i'\in N_k(i)}\mathrm{reachdist}_k(i'\leftarrow i)}\tag{1}$$

$$\mathrm{reachdist}_k(i'\leftarrow i)=\max\{\mathrm{dist}_k(i),\mathrm{dist}(i,i')\}$$

(5) 计算$\mathrm{LOF}_K(i)$

$$\mathrm{LOF}_K(i)=\frac{\sum\limits_{i'\in N_K(i)}\frac{\mathrm{lrd}_k(i')}{\mathrm{lrd}_k(i)}}{\|N_K(i)\|}=\sum_{i'\in N_K(i)}\mathrm{lrd}_k(i')\cdot\sum_{i'\in N_K(i)}\mathrm{reachdist}_k(i'\leftarrow i)\tag{2}$$

(6) 对$\mathrm{LOF}_K(i)$进行排序，剔除LOF高的数据。

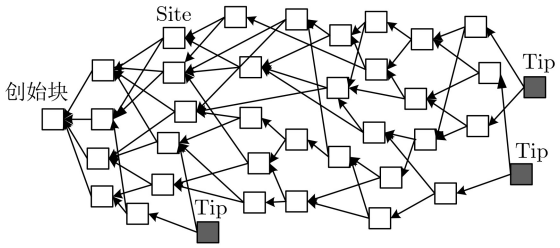

图 2 Tangle网络交易结构

定义3 累计权重 一个交易的累计权重定义为自身的权重加上所有直接或间接指向该交易的所有Site的权重。

定义4 Tip 在Tangle中未被验证过的Site。

3.1　数据发布

若节点N_i要将T_j发布到Tangle网络中，首先需利用马尔科夫蒙特卡洛(Markov Chain Monte Carlo, MCMC)算法选择两个Tips验证(见表2)。验证过程包括交易是否为合法数据，即其是否具有TS的签名，及数据的可靠性和用户签名等功能。其次，节点需要检查T_j在网络中是否存在冲突(即同一份数据被发布两次)。此外，为了防止垃圾邮件等问题，N_i需要做一个小的PoW计算，此时的难度值将会设置成非常低，连接上前两个交易的交易号一起算hash-hash(ida, idb, nounce)。将得到的结果写入当前交易中，得到摘要后4位为0的32 bit字符串。Tangle网络中交易的结构定义如图3所示。

图3中，tag为交易的标签，其具有唯一性，内容与任务相关；timestamp字段用于记录交易时间，若一个交易长期未被验证，节点可重新将该交易数据发布到网络中，或由TS重新选择一个节点完成该任务；address字段记录交易位置；value字段存放交易在Tangle网络中的权重；message字段存储交易信息；sign字段存放节点交易的签名；index和lastIndex字段指向当前交易验证的两个交易；nonce为节点所解决的小pow难题。

节点验证由MCMC算法选择的交易后，以图3的结构将交易同步写入分布式账本，此时称完成了一次交易写入过程。

3.2　酬金交付

为了防止虚假任务发布，任务发布者不仅需将酬金v(包含服务费)上传到PS，同时还需向PS支付一定的押金π_R。即任务发布前，需给平台所有的赎金($\mathrm{deposit}_R=v+\pi_R$)。在任务完成截止时间之前不能被用户赎回。任务发布者可根据任务的重要性对交易权重设定不同的阈值。当交易到达阈值时，平台首先会检查该交易节点的身份，确认后将

表 2 算法2：基于MCMC的端点选择算法

输入：马尔可夫链状态转移矩阵$\boldsymbol{Q}$，平稳分布$\pi(x)$，最大转移次数$n1$，选定时间间隔$[W, 2W]$及该间隔下的样本个数$n2$(此时的样本个数为新到的交易所观察到的交易数目)。

输出：两个最先走到Tip的粒子为新交易将验证的端点。

for t=0 to $n1 + n2$–1:

(1) 初始化马尔可夫链$X_0 = x_0$;

(2) 独立的在该选定的间隔中随机放入N个粒子定义为“Walker”；

(3) 每个粒子根据定义的转移概率P随机的选出一条路径，向着Tip的方向进行游走。其中转移概率定义为：

$$P_{xy} = \frac{\mathrm{e}^{-a(H_x - H_y)}}{\sum\limits_{z:x\leftarrow z} \mathrm{e}^{-a(H_x - H_z)}} \tag{3}$$

其中，$a > 0$，为自定义参数，H_x和H_y为交易x和交易y的累计权重，转移后第t个时刻的马尔可夫链状态为$X_t = x_t$，下一个交易可能的状态为$y_{t+1} = x_t p(x|x_t)$，此时$\pi(x) = (x_{n1}, x_{n1+1}, \cdots, x_{n1+n2-1})$。

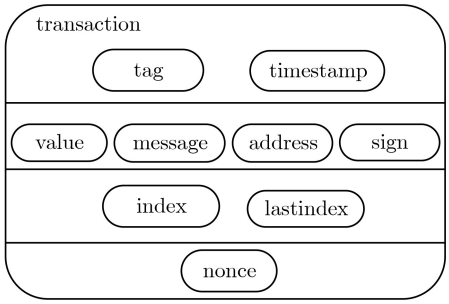

图 3 交易结构

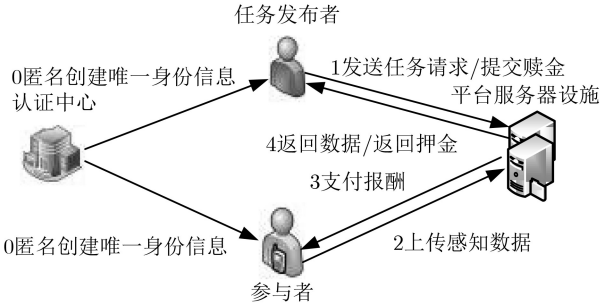

图 4 身份匿名过程

自动执行Tangle网络的智能合约代码，将赎金转账给获胜节点。同时，任务发布者可从TS下载交易数据，此时称完成了一笔数据和酬金的安全交付。

4 Tangle网络隐私安全保证

参与者使用匿名身份对采集到的数据进行签名[14]，身份验证过程在Tangle网络中由新加入的节点确认，且其只能看到前两个交易的匿名身份及其任务号，Tangle网络中所有的交易最终都将以地址作为唯一标识，即任务发布，数据采集完成后交易的认证，以及酬金支付都将按照网络地址进行数据传输。具体认证过程如图4所示。

(1) 初始化(1^λ)：输出密钥管理系统的公钥mpk和私钥msk。其中λ为系统输入参数。

(2) 节点身份证书(msk, pk)：使用管理系统的私钥对参与者的公钥进行签名，产生关于节点身份信息的证书。

(3) 认证(m, sk, pk, cert, mpk)：为了验证一个消息m确实有被认证过的密钥签过名，需对这个消息进行认证，对于消息m调用认证函数输出一个关于消息的证书π。

(4) 验证消息(m, mpk, π)：为验证数据的可靠性，想要加入Tangle网络的节点同时利用从服务器中查询到的关于消息的证书π和系统公钥mpk对交易数据m进行验证。如果该交易通过验证消息函数输出的结果为0，那么新加入的节点将不会验证该交易。

5 仿真试验与分析

在IoTA网络基础上建立群智感知模块应用，Ubuntu Server 18.10系统下搭建TS分发框架，在同一局域网下测试50名Windows系统用户完成50例图像的标记任务。将任务按时间顺序分发到网络中，定义每类任务最多由10名用户完成。

系统扩展IoTA分布式账本，分别完成了服务器和客户端C语言代码。服务器代码包括任务接收，发布，调用LOF算法抛弃离群点等。客户端完成节点生成、操作邻居节点、端点选择、匿名身份检查、交易冲突检查、交易发布。

5.1 安全性分析

(1) 防双花攻击

考虑节点使用MCMC算法进行交易选择之后，会对其进行双花检查，检查过程为追溯所有交易历史，查看该交易的address字段和tag是否重复，若重复则为双花。此时，节点会执行MCMC算法M次，对重复的每笔交易算置信度C，查看交易被间接选择进行验证的次数L，节点会选择置信度高的交易进行验证。

$$C = \frac{L}{M} \times 100\% \tag{4}$$

例如，若节点发现A与B为双花交易，其执行MCMC算法100次，A, B被间接验证的次数分别为97, 3，节点此时将会抛弃B交易，随着新加入网络的交易越来越多，A交易得到验证的次数和累计权重将会越来越大，B交易在其之后将不会被新到的节点验证，证明Tangle网络能够防止双花攻击。

(2) 防DoS攻击

传统群智感知平台中的资金交易信息都需要存储在PS中，若遭受大规模的DoS攻击，可能导致参与者无法及时获取相应酬金。然而本文中所有的交易信息作为分布式账本被存储在各个节点之中，当PS遭到DoS攻击，模型能立刻启动一个可信的备份服务器并从故障中恢复过来。

(3) 防女巫攻击

女巫攻击在Tangle网络中表现为攻击者发布大量的冗余交易，造成网络高度拥塞，导致交易验证速度变慢。而Tangle群智感知网络在节点发布交易之前，需要完成确定的数据采集任务，此过程将会消耗节点大量的算力，使恶意节点不能在短时间内进行女巫攻击。

5.2 隐私保护分析

试验采用GeoLige项目[15]中公开的数据集，数据点为不同频率GPS记录器每隔5～10 min对用户的位置数据进行采集得到。随机选取150个数据点，经过坐标处理转换到2维平面中，赋予每个数据点虚拟的IP地址及身份并模拟成数据交易。试验分析了群智感知过程中可能存在的隐私泄露点，结果如表3所示。

考虑攻击者联合恶意参与者同时竞争相同的任务，关联到合法用户身份并进行攻击。根据表3，试验分析模型在不同参与者数目下隐私泄露的概率。试验结果如图5所示。

表 3　群智感知过程中的隐私泄露点

隐私泄露过程	隐私泄露位置	窃取隐私难易程度
参与者将采集数据上传至TS	参与者与TS通信的中间网络遭受中间人攻击	易
参与者与其他传感器交互	传感器设备	易
交易写入Tangle网络	Tangle网络	易
TS调用LOF算法	TS	中
TS指定获胜节点	TS	中
PS支付酬金	PS	中

图5中3条曲线分别表示攻击者所俘获不同比例合法参与者的情况。当参与者的数量逐渐增加时，由于任务分发采用随机分配原则，参与者可随时更换自己的IP地址。此时假设攻击者不能劫持超过20%的合法参与者，当参与者的数目达到20时，隐私泄露的概率将会小于0.05。

5.3 时间性能分析

数据包含5个训练集和1个测试集，每个集合中包含1000张图片。随机地从训练集中选取50, 100, 150, 200, 250张照片作为任务，分别被标记为task_50, task_100, task_150, task_200, task_250。为方便对比试验，试验设计各类任务的酬金是相同的。

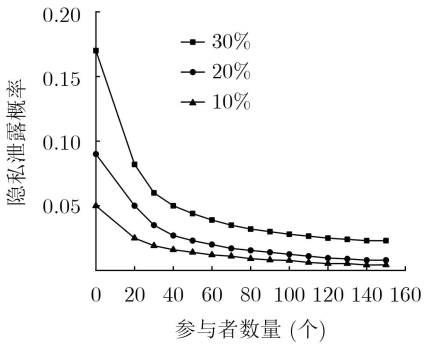

图 5 隐私数据泄露的概率

Tangle网络设置节点计算pow的难度为10 s，假设每个节点具有的算力相同，即每个交易自身的权重都为1，累计权重的阈值为10。其中，一笔交易被确认所需要的平均时间如表4所示，约为30 s。其中图6(a)—图6(c)证明交易越大，其交易发布至交易被验证的时间越长，但其消耗的时间在可控范围内。图6(d)和图6(f)计算了TS选取可靠数据、存储及交换数据所需要的时间。其中各个时间均与数据的大小有关，如表4所示。然而，如果当任务量较小时，可以看到服务器处理各个节点上传的数据所需要的时间基本相同，大约为245.67 ms，图6(e)表明TS接收参与者所上传数据的时间大约需要13.79 ms。

将节点所发布的群智感知数据与任务发布者早先发布的任务进行对比，分析模型在5000张图片的测试集中精度为93.11%。表明模型在保障数据质量的同时降低了时间花销。

5.4 任务成本分析

假定任务发布者为任务支付的平均费用为每标记100张图片14个IoTA币，平均每个IoTA币为

表 4 Tangle网络处理数据的时间花销

名称	任务发布		任务接收		交易上传	
	任务大小(kb)	处理时间(ms)	任务大小(kb)	处理时间(ms)	任务大小(kb)	处理时间(ms)
Task_50	1179.59	489.40	1289.69	4.47	4.7945	245.67
Task_100	2356.45	620.43	2416.15	7.89	9.7255	245.69
Task_150	3552.86	722.71	3932.77	13.79	14.0229	245.65
Task_200	4841.76	905.32	4825.98	11.63	21.3921	245.67
Task_250	5761.84	1219.45	5832.97	18.23	25.7526	478.90

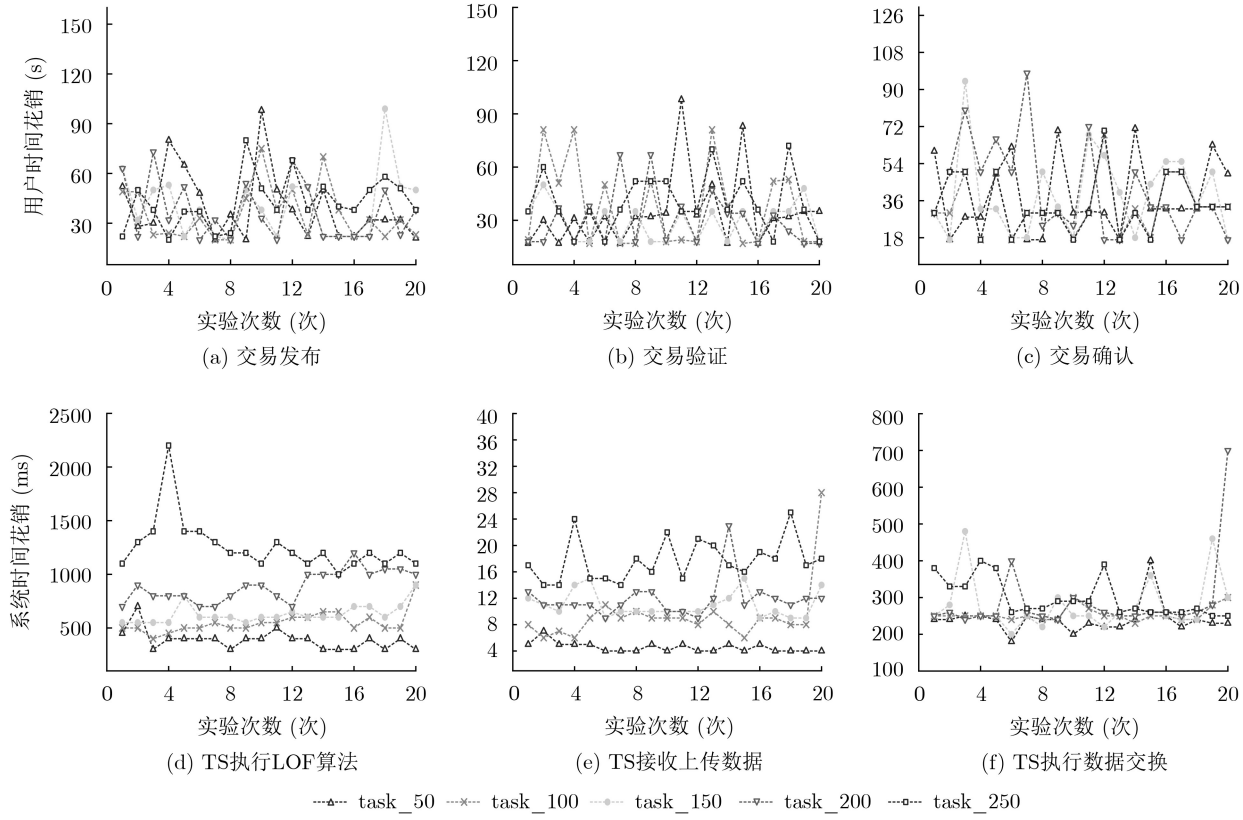

图 6 时间复杂性分析

50$。为便于试验，将本模型简记为TNM与以太坊中的(AMeiToken, AMT)奖励政策机制收取的服务费进行对比，结果如图7所示。

从图7中可以看出， TNM模型的服务费远远低于AMT模型，尤其是在处理大任务时，当需要标记图片的数量为250张时，AMT机制下的服务费增长率比TNM模型高400%。

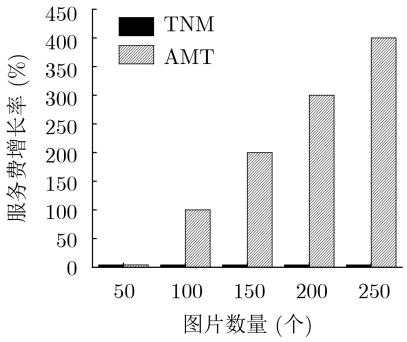

图 7 TNM模型与AMT机制服务费对比

6 结束语

针对现有群智感知中数据交付过程的安全问题，本文提出将Tangle网络作为分布式账本的全新感知数据交付模型。基于区块链的分布式结构和对数据去中心化存储的特性以解决服务器抵赖数据交易及第三方介入带来的安全问题，此外，模型支持身份匿名技术以保障用户隐私。与传统链式结构相比极大地降低了任务发布所需成本。但本文在任务分发环节仅考虑了参与者的位置因素，即认为每个参与者的能力属性均相同，没有综合分析不同参与者针对不同类型任务的可靠性。因此，在今后的研究中，可针对以上问题对模型进行改进，以提高任务完成的质量和效率。

参 考 文 献

[1] 熊金波, 马蓉, 牛犇, 等. 移动群智感知中基于用户联盟匹配的隐私保护激励机制[J]. 计算机研究与发展, 2018, 55(7): 1359–1370. doi: 10.7544/issn1000-1239.2018.20180080.
XIONG Jinbo, MA Rong, NIU Ben, *et al*. Privacy protection incentive mechanism based on user-union matching in mobile crowdsensing[J]. *Journal of Computer Research and Development*, 2018, 55(7): 1359–1370. doi: 10.7544/issn1000-1239.2018.20180080.

[2] 崔勇, 宋健, 缪葱葱, 等. 移动云计算研究进展与趋势[J]. 计算机学报, 2017, 40(2): 273–295. doi: 10.11897/SP.J.1016.2017.00273.
CUI Yong, SONG Jian, Miao Congcong, *et al*. Mobile cloud computing research progress and trends[J]. *Chinese Journal of Computers*, 2017, 40(2): 273–295. doi: 10.11897/SP.J.1016.2017.00273.

[3] 何云华, 李梦茹, 李红, 等. 群智感知应用中基于区块链的激励机制[J]. 计算机研究与发展, 2019, 56(3): 544–554. doi: 10.7544/issn1000-1239.2019.20170670.
HE Yunhua, LI Mengru, LI Hong, *et al*. A blockchain based incentive mechanism for crowdsensing applications[J]. *Journal of Computer Research and Development*, 2019, 56(3): 544–554. doi: 10.7544/issn1000-1239.2019.20170670.

[4] HUANG Kuanlun, KANHERE S S, and HU Wen. Preserving privacy in participatory sensing systems[J]. *Computer Communications*, 2010, 33(11): 1266–1280. doi: 10.1016/j.comcom.2009.08.012.

[5] DONG Kai, GU Tao, TAO Xianping, *et al*. Privacy protection in participatory sensing applications requiring fine-grained locations[C]. The 16th IEEE International Conference on Parallel and Distributed Systems, Shanghai, China, 2010. doi: 10.1109/ICPADS.2010.127.

[6] CHRISTIN D, GUILLEMET J, REINHARDT A, *et al*. Privacy-preserving collaborative path hiding for participatory sensing applications[C]. The 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Valencia, Spain, 2011: 341–350. doi: 10.1109/MASS.2011.41.

[7] 徐哲, 李卓, 陈昕. 面向移动群智感知的多任务分发算法[J]. 计算机应用, 2017, 37(1): 18–23, 47. doi: 10.11772/j.issn.1001-9081.2017.01.0018.
XU Zhe, LI Zhuo, and CHEN Xin. Multi-task assignment algorithm for mobile crowdsensing[J]. *Journal of Computer Applications*, 2017, 37(1): 18–23, 47. doi: 10.11772/j.issn.1001-9081.2017.01.0018.

[8] CHRISTIN D, ROßKOPF C, HOLLICK M, *et al*. IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications[J]. *Pervasive and Mobile Computing*, 2013, 9(3): 353–371. doi: 10.1016/j.pmcj.2013.01.003.

[9] RESTUCCIA F and DAS S K. FIDES: A trust-based framework for secure user incentivization in participatory sensing[C]. IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks 2014, Sydney, Australia, 2014: 1–10.

[10] CHANG S H, CHEN Y S, and CHENG S M. Detection of Sybil attacks in participatory sensing using cloud based trust management system[C]. 2013 International Symposium on Wireless and Pervasive Computing, Taipei, China, 2013: 1–6. doi: 10.1109/ISWPC.2013.6707448.

[11] LI Ming, WENG Jian, YANG Anjia, *et al*. CrowdBC: A blockchain-based decentralized framework for crowdsourcing[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2019, 30(6): 1251–1266. doi: 10.1109/TPDS.2018.2881735.

[12] LU Yuan, TANG Qiang, and WANG Guiling. ZebraLancer: Crowdsource knowledge atop open blockchain, privately and anonymously[J]. arXiv: 1803.01256v4, 2018.

[13] 严云洋, 瞿学新, 朱全银, 等. 基于离群点检测的分类结果置信度的度量方法[J]. 南京大学学报: 自然科学, 2019, 55(1): 102–109. doi: 10.13232/j.cnki.jnju.2019.01.010.
YAN Yunyang, QU Xuexin, ZHU Quanyin, *et al*. Confidence measure method of classification results based on outlier detection[J]. *Journal of Nanjing University: Natural Science*, 2019, 55(1): 102–109. doi: 10.13232/j.cnki.jnju.2019.01.010.

[14] 张俊松, 甘勇, 贺蕾. 群智感知环境下支持激励机制实施的匿名身份认证协议研究[J]. 小型微型计算机系统, 2018, 39(7): 1522–1526. doi: 10.3969/j.issn.1000-1220.2018.07.027.
ZHANG Junsong, GAN Yong, and HE Lei. Anonymous authentication protocol for supporting incentive mechanism in crowd sensing[J]. *Journal of Chinese Computer Systems*, 2018, 39(7): 1522–1526. doi: 10.3969/j.issn.1000-1220.2018.07.027.

[15] JUNG T, LI Xiangyang, and WAN Meng. Collusion-tolerable privacy-preserving sum and product calculation without secure channel[J]. *IEEE Transactions on Dependable and Secure Computing*, 2015, 12(1): 45–57. doi: 10.1109/TDSC.2014.2309134.

赵国生：男，1977年生，博士，教授，研究方向为可生存技术、认知网络、可信计算.

张　慧：女，1994年生，硕士生，研究方向为群智感知.

王　健：女，1979年生，博士，教授，研究方向为SDN、可生存技术、认知网络、群智感知.