SCMA mMTC 系统中基于联盟区块链的无线电资源交易的信用支付

孙 君[1],熊 关[2]
(1. 南京邮电大学江苏省无线通信重点实验室,江苏南京 210003;2. 南京邮电大学通信与信息工程学院,江苏南京 210003)

摘 要: 无线电资源交易发生在 MTC 网关(MTC Gateway MTCG)和 LTE 用户之间. 根据基于联盟区块链的空闲无线电资源交易来建立 MTCG 之间的信用度. 在多个授权的本地基站(Base Station BS)上建立了一个联盟区块链,用于公开审计和共享交易记录. 资源交易记录在加密后上传到 BS. 在交易记录通过审查和共识过程之后,新区块被存储在 BS 上,并且可以由 MTCG,LTE 用户和连接到联盟区块链的 BS 进行公开访问. 为了最大化系统的利益,支持频繁的资源交易,提出了一种基于信用贷款的支付方案,并给出了相应的最优定价策略.

关键词: 联盟区块链; 信用贷款; 无线电资源信用交易; 信用度
中图分类号: TN929. 5 **文献标识码:** A **文章编号:** 0372-2112 (2019)08-1677-08
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2019. 08. 010

Credit Payment for Radio Resources Transactions Based on Consortium Blockchain in SCMA mMTC

SUN Jun[1], XIONG Guan[2]
(1. *Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Jiangsu, Nanjing* 210003, *China*;
2. *College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Jiangsu, Nanjing* 210003, *China*)

Abstract: The radio resources trading happened between the MTCGs and the LTE users. The credit degrees are built among the MTCGs according to the free radio resources trading based on the consortium blockchain. A consortium blockchain has been established on the BSs for publicly auditing and sharing of transaction records without depending on the trusted third parties. The resource transaction records are uploaded to the BS after encryption. After the transaction records pass the review and consensus process, the new blocks are stored on the BSs that can be accessed publicly by MTCGs, LTE users and the BSs connected to the consortium blockchain. In order to maximize the benefits of the system and support frequent resource transactions, a credit-based payment scheme and the corresponding optimal pricing strategy are proposed.

Key words: consortium blockchain; credit loan; credit radio resources trading; credit degrees

1 引言

大规模机器类通信场景(mMTC)是第五代(5G)无线通信系统的三种应用场景之一. 它应该支持数百亿低复杂度,低功耗的机器类型设备(MTC Device MTCD)的连接. 为了应对这一挑战,未来的网络可能会采用 MTC 网关(MTCG)作为网络的接入点,使用 MTC 设备作为中继和在基站进行服务质量(QoS Quality of service)聚类[1]. 通过使用 MTCG,网络将变成一个双层结构,MTCG 将协调集群中的 MTCD 并通过两跳链路访问网络. MTCD 可以采用稀疏编码多址接入技术[2]接入到 MTCG 中,进一步提高系统性能.

由于无线频谱资源有限,优化上述双层网络系统中的无线资源分配以提高系统性能至关重要. 基于 mMTC 的场景特性,MTCG 转发的数据流量大小与一个 LTE 用户传输的数据流量大小基本一致. 由认知无线电[3]的原理可知,获得某一频段授权的 LTE 用户对该频段拥有优先使用权,而当该 LTE 用户不进行数据传输时,可以将空闲的授权频段出让或租赁给其他有频谱资源需求的用户. 因此,可以开发一个频谱资源交易

收稿日期:2018-09-27;修回日期:2019-04-12;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61771255, No. 61427801)

系统,进一步对 MTCG 与小基站相连的上层网络系统进行优化. 联盟区块链是一种特定的区块链,具有多个授权节点,可以以适中的成本建立分布式共享账本[4]. 5G 中的低频资源主要用于连续广覆盖、低时延高可靠、低功耗大连接等应用场景. 针对部署在高频高容量热点区域,主要应用微蜂窝,即以小基站为基本载体. 对于 mMTC 应用场景,可能会采用在单个宏蜂窝小区的热点区域部署小基站,以增强连接,进一步扩大网络容量,减轻宏基站的连接负担. 因此,小基站(BS)可以充当授权节点,MTCG 和 LTE 用户作为资源交易的买卖双方,基于联盟区块链技术开发一个安全的本地化 P2P 频谱资源交易系统. 在 BSs 上建立了一个联盟区块链,用于公开审核和共享交易记录,而不依赖于受信任的第三方中介. 买卖双方之间的资源交易记录在加密后上传到 BS,这些交易记录通过审核和共识流程后,构成新的区块存储在 BSs 上,并且可以由 MTCGs,LTE 用户和连接到联盟区块链的 BS 公开访问. 此外,提出了一种基于信用贷款的支付方案,以支持频繁的频谱资源交易. 在所描述的 mMTC 应用场景中,一般情况下,MTCG 承担的角色是频谱资源购买用户,LTE 用户则根据实际的业务场景和实时状态选择相应的角色.

通过构造基于联盟区块链的频谱资源交易系统,可以有效地利用系统中闲置的频谱资源,进一步提高系统的资源利用率. 在传统的认知无线电中,认知用户需要进行两个阶段:频谱感知和认知传输阶段. 在频谱感知阶段,认知用户需要根据频谱检测设备收集频谱信息. 在认知传输阶段,认知用户检测到空闲频谱后,选择最佳的频谱进行通信传输. 与传统的认知无线电频谱交易系统[5]相比,所构造的基于区块链技术的频谱资源交易系统有以下优点:

(1)在传统认知无线电频谱交易系统中,一般情况下,系统采用的集中式的网络结构[6],并且会引入一个可信的第三方中介来审核和验证交易记录,容易遇到单点故障. 而我们所设想的基于联盟区块链的频谱交易系统中,采用的是分布式的网络存储技术,并且区块链相关技术的引入提高了安全性.

(2)在传统认知无线电频谱交易系统中,在频谱感知阶段,认知用户需要根据频谱检测设备收集频谱信息. 而基于区块链的频谱交易系统中,无需搭设额外的频谱检测设备,极大地节约了成本.

本文的主要贡献有两方面:

(1)基于信用贷款的支付方案:为了使上述基于联盟区块链的频谱资源交易系统没有足够资源货币的资源购买用户也能完成相应的资源交易,提出了一种基于信用贷款的支付方案,以支持频繁的资源交易,促进本地网络的频谱资源交易.

(2)最优定价策略:对于基于信用贷款的支付方案,提出了基于信用贷款的最优定价策略,以最大化信用银行的效用. 数值结果表明,基于信用的支付方案是有效的.

2 基于联盟区块链的无线电资源交易系统概述

如图 1 所示,为了扩大网络容量,针对于 mMTC 应用场景,在单个宏蜂窝小区的热点区域部署小基站. 小基站可以充当授权节点,MTCG 和 LTE 用户作为资源交易的买卖双方,基于联盟区块链技术开发一个安全的本地化 P2P 无线电资源交易系统.

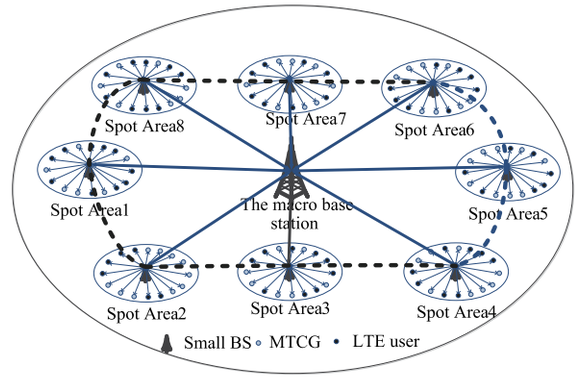

图1 小区双层网络分布图

2.1 资源交易模型中的实体

如图 2 所示;基于区块链的无线电资源交易模型主要包括以下实体.

(1)资源购买用户与资源出售用户:MTCGs 和 LTE 用户依据具体的业务特性所确定的频谱资源需求和当前所拥有的频谱资源状态选择自己的角色,分别来充当频谱资源交易中的买方和卖方.

(2)小基站:在小区中的热点区域,小基站可以作为资源经纪人. 在整个交易系统中,一种名为资源货币的数字加密货币作为用户的数字资产. 每个资源出售用户向最近的小基站发送资源出售的请求,包括空闲频谱资源信息和出售价格. 资源经纪人对本地空闲资源出售请求进行统计,并向资源购买用户广播该请求. 资源购买用户向资源经纪人提交购买资源数量和资源购买价格. 资源经纪人协调买卖双方之间的交易. 作为资源经纪人的小基站包含了 4 个实体,即:交易服务器,信用银行,账户池和内存池. 交易服务器从资源购买用户中收集资源购买请求,并匹配资源交易的最佳买卖双方用户. 交易服务器还控制着出售的频谱资源的接入,以完成买卖双方之间的频谱资源交易. 每一个用户都有一个资源货币账户,用于存储用户交易记录,同时有一个相应的钱包来管理该账户中的资源货币. 所有

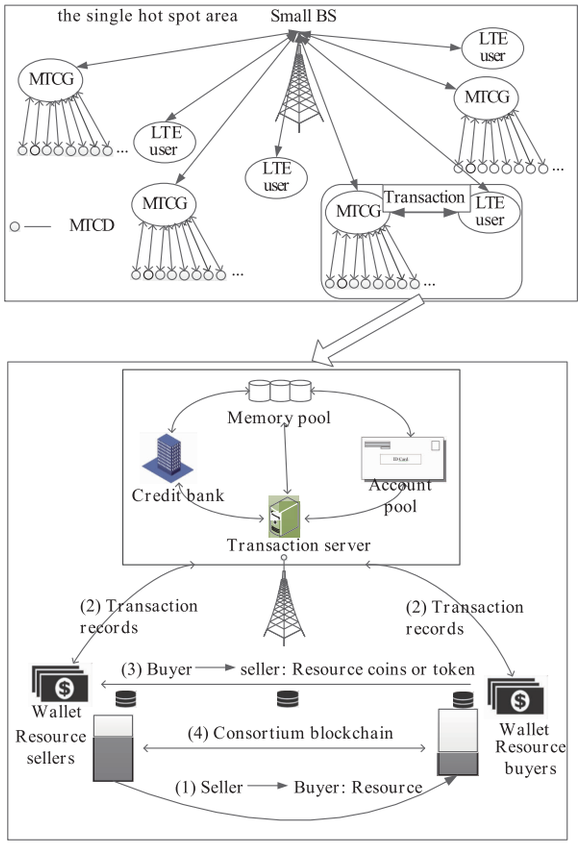

图2　基于区块链的无线电资源交易模型

钱包地址,以及钱包和账户之间的映射关系都存储在账户池中. 内存池存储着所有本地用户的交易记录.

(3)频谱资源计算和存储:部署在热点区域的小基站具备频谱资源计算功能,可以实时地计算频谱资源交易数量,存储频谱资源交易记录. 资源购买用户根据小基站中的交易记录向资源出售用户进行支付.

2.2　资源交易模型中的操作细节

为了保证 P2P 频谱资源交易的安全性,我们利用联盟区块链建立无线电资源交易模型. 在传统区块链中,交易记录在形成区块链之前必须执行名为共识过程的重要交易审计阶段. 该阶段由传统区块链中的所有验证节点以高成本执行. 与传统区块链不同,联盟区块链以适中的成本对预先选择的校验节点执行共识过程. 在构造联盟区块链时,将预先选择的小基站作为校验节点. 同时这些小基站收集和管理其本地交易记录. 在完成所选择的小基站之间的共识过程之后,这些交易记录被构造成区块,并存储在内存池中. 资源交易模型中的操作细节如下所示:

(1)系统初始化:在联盟区块链中,利用椭圆曲线数字签名算法和非对称加密技术进行系统初始化[6]. 每个用户首先在可信任的权威管理机构上进行注册,成为一个合法实体. 用户 i 在注册之后加入系统并获得私钥,公钥以及相应的证书(表示为 SK_i,PK_i 和 $Cert_i$),其中用户的真实身份标识为 ID_i. 证书 $Cert_i$ 可通过绑定用户的注册信息(如真实身份标识 ID_i)来唯一地识别用户. 用户 i 从可信任的权威管理机构获得 v 个钱包的地址集合 $\{WID_{i,k}\}_{k=1}^{v}$,同时生成一个映射列表 $\{PK_i, SK_i, Cert_i, \{WID_{i,k}\}_{k=1}^{v}\}$. 当用户 i 执行初始化时,用户 i 将钱包地址和映射列表上传到离它最近的 BS 的账户池,并通过内存池下载有关其钱包的最新数据.

(2)角色选择:在频谱资源交易中,MTCGs 和 LTE 用户依据具体的业务特性所确定的频谱资源需求和当前所拥有的频谱资源状态选择自己的角色,分别来充当频谱资源交易中的买方和卖方. 具有闲置频谱资源的用户可能成为频谱资源出售用户,以满足频谱资源购买用户的频谱需求.

(3)频谱资源交易数量与价格的确定:资源出售用户向 BS 的交易服务器发送频谱资源出售请求,包括空闲频谱资源信息和出售价格. 交易服务器统计本地空闲资源出售请求,并向资源购买用户广播该请求. 资源购买用户确定其购买的频谱资源数量和购买价格并给交易服务器返回响应. 交易服务器匹配买卖双方用户之间的频谱资源供需关系,确定最佳的频谱资源出售数量,以及最佳售价.

(4)使用资源货币进行付款:在频谱资源交易后,有足够资源货币的资源购买用户通过使用资源出售用户的钱包地址进行支付,即资源购买用户将资源货币从其钱包转移到资源出售用户的钱包地址. 没有足够资源货币的资源购买用户可以根据其自身的信用等级从信用银行申请信用贷款,来完成支付. 关于信用贷款,更多细节见第三节. 资源出售用户可以从 BS 的内存池中获取最新的区块数据以验证该支付的正确性. 在完成支付后,资源购买用户产生新的交易记录. 这些交易记录由资源出售用户验证并对其进行数字签名,同时将这些记录上传到 BS 中进行审核.

(5)联盟区块链中的区块构造:在完成支付后,每一笔交易记录会上传到 BS 的内存池中,每个授权 BS 会从中选取若干个交易记录构建成一个区块. 首先授权 BS 对区块中的交易记录进行数字签名,即将交易记录进行哈希,得到摘要,再用私钥对摘要进行加密得到数字签名,并将数字签名附在交易记录的后面. 每个区块包含区块链中先前区块的哈希值以及数字签名. 其次其他授权 *BS* 在接收到该区块后利用发送者的公钥对数字签名进行验证,以保证数据在在传播路径上未被篡改过,确保数据的完整性. 最后其他授权 BS 对该区块执行共识流程. 授权 BS 通过共识算法对该区块的合法性进行校验,通过校验后,所有授权 BS 将该区块

添加区块链中.

(6)共识流程的执行:该联盟区块链采用 PBFT 算法[7-8]作为共识算法. 这里假设在区块链系统中共有 3F+1 个授权 BS,一个 Quorum 至少包含 2F+1 个授权 BS. 共识流程由授权的 BS 执行,一共分为三个阶段. 当某一 BS 满足生产区块条件时,该 BS 生成 Pre-Prepare 证书,并将该证书发送给其他授权 BS 之后,该 BS 进入 Prepare 状态. 其他授权 BS 在收到该 BS 的 Pre-Prepare 证书,即在收到了新生成区块信息时进入 Prepare 状态. 当这些授权 BS 检测到 Pre-Prepare 证书来自生成新区块的 BS 时并且是第一次接收时,会将 Prepare 证书进行广播,并记录证书信息. 当每个授权 BS 检测到某一个 Prepare 证书通过 2F 个授权 BS 同意时,对于该证书,每个授权 BS 会接收到其他授权 BS 的 Commit 信息. 当检测到该 Commit 信息经过 2F+1 个授权 BS 同意时,则认为该区块信息在系统中达到共识.

3 基于信用贷款的支付方案

在频谱资源交易后,没有足够资源货币的资源购买用户则无法通过使用资源出售用户的钱包地址进行支付,导致整个资源交易无法完成. 由于资源出售用户的空闲资源不能得到有效的利用和资源购买用户的购买需求无法及时得到满足,从而导致整个资源交易系统的效率较低. 为了解决这个问题,进一步促进资源交易,提高空闲频谱资源利用率,提出了一种基于信用贷款的支付方案来支持频繁的频谱资源交易. 假设每个授权 BS 中的信用银行具有足够资源货币提供给贷款用户.

在频谱资源交易后,有足够资源货币的资源购买用户通过使用资源出售用户的钱包地址进行支付,即资源购买用户将资源货币从其钱包转移到资源出售用户的钱包地址. 没有足够的资源货币的资源购买用户可以根据其自身的信用等级从信用银行申请信用贷款,来完成支付. 因此当资源购买用户拥有足够的资源货币支付给资源出售用户时,则无需可信中介参与交易;当资源购买用户需要借助基于信用贷款的支付方案完成支付,则需要依赖 BS 完成信用贷款. 在本文中主要是提出了一种基于信用贷款的支付方案来促进本地网络的频谱资源交易,使得本身没有足够资源货币的资源购买用户也能完成相应的资源交易. 关于该支付方案的安全性优势将在第五节进行讨论. 如图 3 所示,信用银行根据贷款用户的信用度为该用户提供资源货币贷款,然后将资源货币从信用银行账户转移到信用银行和贷款用户之间共享的钱包地址,最后依据贷款用户的交易信息,将资源货币从共享钱包地址转移到资源出售用户的钱包地址完成支付. 我们采用信用等级因子对信用度进行定义,更多细节在第四节中进行描述.

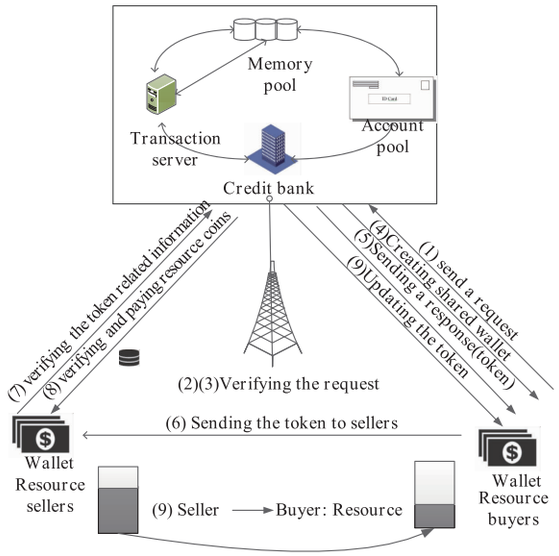

图3 基于信用贷款的支付方案

关于基于信用贷款的支付方案的操作细节如下.

(1)借贷请求:当资源购买用户 MR_i 没有足够的资源货币完成支付时,则该用户充当贷款用户 DB_i 的角色,可以根据其自身在本地信用银行的信用值来申请贷款以完成支付. 具体步骤如下所示.

(a) **Step1**:DB_i 向 BS_n 发送包括真实身份 ID_i,证书 $Cert_i$,所有使用的钱包地址 $\{WID_{i,k}\}_{k=1}^{v}$,贷款金额 AM_i 和当前信用值 CR_i 的请求($request_i$),即 $DB_i \rightarrow BS_n$:$request_i = \{ID_i \| \{WID_{i,k}\}_{k=1}^{v} \| Cert_i \| CR_i \| AM_i\}$.

(b) **Step2**:在接收到 $request_i$ 后,信用银行依据 BS_n 中的账户池和信用银行中的记录来验证 DB_i 的合法性,并检查给定钱包地址 $\{WID_{i,k}\}_{k=1}^{v}$ 的资金流,并获取 DB_i 当前的财富值.

(c) **Step3**:当以下条件成立时,DB_i 获得贷款:(i) DB_i 的资源货币账户中有一些财富;(ii) DB_i 的信用值大于信用贷款的信用阈值. 信用银行计算 DB_i 的最佳贷款金额,相应的利率和罚款率.

(d) **Step4**:信用银行创建共享钱包(SW_{cb}^{i})并将该钱包的公钥和私钥(即 PK_{cb}^{i} 和 SK_{cb}^{i})发送给 DB_i. PK_{cb}^{i} 是信用银行 BS_n 和 DB_i 共享的钱包地址. 当 DB_i 满足贷款条件时,DB_i 可以使用 SW_{cb}^{i} 中的资源货币来完成支付.

DB_i 接收来自信用银行的响应,即 $BS_n \rightarrow DB_i$:$response_i = \{(PK_{cb}^{i}, SK_{cb}^{i}) \| Token_i \| Sign_{SK_{cb}}(Token_i) \| Timestamp\}$. 其中 $Token_i = \{BA_i \| t \| Buffer \| Cert_{cb} \| Cert_{cb}^{i} \| AM_i \| pre\_redord_i\}$,$pre\_redord_i = \{PR_i(s,f) \| Hash(TX_i)\}$. 信用银行利用自身的私钥 SK_{cb} 对 $Token_i$ 进行数字签名,得到 $Sign_{SK_{cb}}(Token_i)$.

其中,BA_i为当前余额,AM_i为贷款金额,t 为共享钱包的有效期. *buffer* 为贷款的还款缓冲区,DB_i应该在还款缓冲区偿还资源货币贷款,否则,DB_i将遭受罚款的处罚,同时 DB_i的信用值也会相应的减少. pre_recode_i为之前的贷款记录. pre_record_i包括贷款偿还记录 $PR_i(s,f)$和基于信用贷款的支付记录的哈希值 $Hash(TX_i)$. 在 $PR_i(s,f)$中,s 是之前贷款记录中在还款缓冲区及时偿还贷款的次数,而 f 是未能及时偿还贷款的次数.

(2)支付:在资源交易期间,DB_i使用 SW^i_{cb}中的资源货币来完成支付. 基于信用贷款的每笔付款均由本地信用银行进行验证和记录. 信用银行将支付的相关数据的哈希值放入 pre_record_i中,以便在必要时检查 $\{WID_{i,k}\}_{k=1}^{v}$的资金流. 关于支付操作的具体步骤如下所示.

(a)**Step**1:贷款用户 DB_i向资源出售用户 LR_j发出支付请求($pay\_request$),包括 $Token_i$,$Token_i$的签名和授权证书($Cert^i_{cb}$). LR_j在 $Token_i$中验证授权证书和共享钱包的有效期,并检查区块链中 DB_i之前基于信用贷款的支付记录,确认共享钱包的余额.

$$DB_i \rightarrow LR_j: pay\_request = \{ Token_i \| Sign_{SK_i}(Token_i) \| Cert_i \| Cert^i_{cb} \| Timestamp \}$$

(b)**Step**2:资源出售用户 LR_j向信用银行发送资源账单响应. $LR_j \rightarrow BS_n$: $bill\_response = \{ pay\_request \| Sign_{SK_j}(pay\_request) \| Cert_i \| bill_j \| Timestamp \}$. 该响应包括资源交易账单($bill_j$),资源出售用户的钱包地址($WID_j$),$pay\_request$ 和 $pay\_request$ 的签名. 信用银行将 $pay\_request$ 中接收的 $Token_i$与原始 $Token_i$进行验证,确保其正确性. 如果信用银行中的共享钱包有充足的余额以完成支付,信用银行根据资源交易账单将共享钱包中相应金额的资源货币转移到资源出售用户的钱包地址. 如果信用银行中的共享钱包中的余额不足,信用银行会向 DB_i发送共享钱包余额不足的通知.

(c)**Step**3:在完成支付后,信用银行更新共享钱包 SW^i_{cb}和 $Token_i$的余额信息,并将其数字签名添加到最新的 $Token_i$中.

(3)资源货币贷款的偿还:在 $Token_i$中的有效期 t 过期之后,DB_i接收到信用银行发送的最新 $Token_i$. 最新的 $Token_i$包含所有基于信用贷款的支付记录的哈希值. 如果 DB_i在其还款缓冲区内偿还资源货币贷款,则 DB_i将贷款的利率作为交易费用偿还给信用银行. 利率在第四节中计算. 如果 DB_i无法及时偿还贷款,则中 $RP_i(s,f)$的 f 将加 1. 贷款用户的信用值将减少,贷款用户的新信用值表示为:$CR^i_{n+1} = CR^i_n - d \cdot AM_i$,其中 CR^i_n是第 n 次资源交易的信用值[9]. d 是常数,$d > 0$. 信用银行生成有关此事件的记录,因此将记录存储在内存池中并将其上传到区块链中. 当贷款用户最终偿还资源货币贷款时,DB_i仍然受到罚款的惩罚. 如果 DB_i拒绝偿还贷款或在很长一段时间内无法偿还贷款,信用银行将把贷款用户 DB_i列入黑名单,并将此信息广播到区块链中的所有用户. 所有用户和信用银行将拒绝与贷款用户 DB_i合作.

4　信用贷款中最优贷款金额

4.1　问题建模

本节主要介绍资源购买用户在使用基于信用贷款的支付方案时,信用银行的最优贷款金额和利率问题. 在本地 BS_n中,对于贷款用户 DB_i,由信用银行 CB_n提供的贷款金额表示为 Q_i. 其中 $DB_i \in B$,B 为贷款用户集合. DB_i的最小频谱资源需求表示为 $M_i^{\min}$,p_i是贷款请求之前的给定的资源交易价格. 假设当地信贷银行有足够的资源货币来支持贷款用户的交易支付. DB_i的满意度函数表示为:

$$d_{sat} = e_i \ln\left[k_i\left(\frac{Q_i}{p_i} - M_i^{\min}\right) + 1\right] + w \tag{1}$$

其中 e_i,k_i和 w 均为 DB_i的预定义因子,且有 $e_i > 0$. DB_i的效益函数为:

$$d_i = g_i(d_{sat} - \theta_i Q_i t_i) - (1 - g_i)u_i Q_i \tag{2}$$

其中 g_i是 DB_i可以在还款缓冲区内偿还贷款的概率. g_i可以通过 DB_i的贷款偿还记录 $RP_i(s,f)$来计算,即有 $g_i = s/(s+f)$. θ_i是信用银行的贷款利率,u_i是还款延迟的罚款率. 利率与罚款率之间的关系是 $u_i = \kappa_i t_i \theta_i$[10],$\kappa_i > 1$ 是预定义因子,并且 $t_i > 0$ 是还款缓冲区的时间,信用银行的开销为 $Q_i t_i c_i$,其中 c_i是信用银行贷款的单位成本. 因此,信用银行的经济利益定义如下.

$$d^i_{cb} = \phi_i Q_i t_i(\theta_i - c_i) + (1 - \phi_i)u_i Q_i \tag{3}$$

其中ϕ_i是预定义信用等级因子,取决于信用银行给出的 DB_i的信用等级($0 < \phi_i \leqslant 1$). ϕ_i是根据 DB_i的贷款记录计算得出的. 信用等级越高,ϕ_i越高. 关于ϕ_i值的更多细节在第五节中给出.

竞争的 Stackelberg 博弈中通常会研究多个独立决策者的多级决策过程,以响应博弈中领导者的决策[11]. 引用文献[11]中所提出的竞争的 Stackberg 博弈模型,其中信用银行是领导者,贷款用户是追随者. 信用银行最终得到的解决方案是确定贷款用户的罚款率 u_i,进一步通过$\theta_i = u_i/\kappa_i t_i$确定贷款利率. 每个贷款用户根据信用银行给出的罚款率和贷款利率得到最佳贷款金额. 博弈模型 H 的形式定义为:

$$H = \{B \cup \{CB_m\}, \{d_i\}_{i \in I}, \{d^i_{cb}\}_{i \in I}, Q_i, u_i\} \tag{4}$$

本地 BS 中的信用银行 CB_n和贷款用户的目标函数 DB_i分别表示如下.

$$\begin{aligned} CB:&\max_{u_i}\sum_{i=1}^{I} d_{cb}^{i}(u_i)\\ &\text{s.t.},\ u_i\geq 0\\ DB:&\max_{Q_i} d_i(Q_i)\\ &\text{s.t.},\ Q_i\geq M_i^{\min}p_i-\frac{p_i}{k_i}\end{aligned} \tag{5}$$

4.2 解决方案

使用反向归纳法来解决上述问题的 Stackelberg 均衡[12]. 首先确定 DB_i 的最优贷款金额问题,然后由信用银行确定最优贷款利率和罚金率.

对于 DB_i,有:

$$\frac{\partial d_i}{\partial Q_i}=\frac{g_i e_i}{k_i(Q_i-p_i M_i^{\min})+p_i}-g_i\theta_i t_i-(1-g_i)u_i \tag{6}$$

$$\frac{\partial^2 d_i}{\partial Q_i^2}=-\frac{g_i e_i}{k_i(Q_i-p_i M_i^{min}+f_i p_i)^2}<0 \tag{7}$$

其中,$f_i=1/k_i$. 由公式(7)可知 d_i 是一个严格的凹函数[13]. 我们通过如下求解 $\partial d_i/\partial Q_i=0$ 来获得最优贷款金额.

$$Q_i^{*}=\frac{g_i e_i}{k_i[g_i\theta_i t_i+(1-g_i))u_i]}+p_i M_i^{\min}-f_i p_i \tag{8}$$

将公式(8)代入(3)中,可得:

$$d_{cb}^{i}=\frac{h_1\theta_i+h_3 u_i-h_2}{k_i[g_i\theta_i t_i+(1-g_i)u_i]}+h_4\theta_i-h_5+h_6 u_i \tag{9}$$

其中有:$h_1=g_i e_i\phi_i t_i$,$h_2=g_i e_i\phi_i t_i c_i$,$h_3=g_i e_i(1-\phi_i)$,$h_4=(p_i M_i^{\min}-f_i p_i)\phi_i t_i$,$h_5=(p_i M_i^{\min}-f_i p_i)\phi_i t_i c_i$,$h_6=(p_i M_i^{\min}-f_i p_i)*(1-\phi_i)$. 通过对 d_{cb}^{i} 的单调性进行分析可知,d_{cb}^{i} 首先增加,然后随着 u_i 的增加而减小. 并且有:$p_i M_i^{\min}-(p_i/k_i)<0$ 时,$u_i<0$,即 $u_i^{*}=0$. 进一步可得:

$$\frac{\partial^2 d_{cb}^{i}}{\partial u_i^2}=-\frac{2h_2\kappa_i}{k_i(g_i+\kappa_i-g_i\kappa_i)}<0 \tag{10}$$

由公式(10)可知 d_{cb}^{i} 是一个严格的凹函数. 通过求解 $\partial d_{cb}^{i}/\partial u_i=0$ 来获得最优罚款率 u_i^{*},并可以由 $\theta_i^{*}=u_i^{*}/t_i\kappa_i$ 得到最优贷款利率 κ_i^{*}.

$$u_i^{*}=\sqrt{-\frac{h_2\kappa_i^2 t_i}{(g_i+\kappa_i-g_i\kappa_i)(h_4+k_i h_6\kappa_i t_i)}},(M_i^{\min}p_i-(p_i/k_i)\geq 0) \tag{11}$$

为了实现 Stackelberg 均衡,信用银行需要与每个贷款用户进行交互. 算法 1 迭代地实现博弈中的唯一 Stackelberg 均衡.

算法 1 最优贷款定价算法(Optimal Loan Pricing Algorithm)

1:初始化:$d_{cb}^{i*}=0$,$d_i^{*}=0$,$Q_i^{*}=0$,$u_i^{*}=0$
2:**for** u_i 从 $0\sim u_i^{\max}$ 取值 **do**
3: **for** $\forall i\in I$ do
4: **if** $M_i^{\min}p_i-\frac{p_i}{k_i}>0$ **then**
5: $Q_i^{*}=0$,$u_i^{*}=0$
break
6: **end if**
7: 贷款用户 DB_i 根据公式(8)更新它的贷款金额 Q_i
8: **end for**
9: 信用银行依据公式(3)更新它的效益 d_{cb}^{i*}
11: **if** $d_{cb}^{i}\leq d_{cb}^{i*}$ then
12: $d_{cb}^{i*}=d_{cb}^{i}$,$d_i^{*}=d_i$,$Q_i^{*}=Q_i$,$u_i^{*}=u_i$
13: end if
14: if $d_{cb}^{i}\leq d_{cb}^{i*}$ **then**
break
15: **end if**
15:**end for**
16:**Output**:d_{cb}^{i*},d_i^{*},Q_i^{*},u_i^{*}

5 仿真结论分析和安全分析

5.1 安全性分析

与传统的认知无线电交易模型的支付手段不同,上述基于信用贷款的支付方案利用基于联盟区块链技术的无线电资源交易系统确保资源交易的隐私安全. 关于基于信用贷款的支付方案和整个无线电资源交易系统安全性能的描述如下所示;

(1)不依赖于可信的中介:在无线电资源交易模型中,与传统的依赖于可信中介的集中式交易方式不同,用户节点以 P2P 的方式进行交易. 当资源购买用户拥有足够的资源货币支付给资源出售用户时,则无需可信中介参与交易;当资源购买用户需要借助基于信用贷款的支付方案完成支付,则需要依赖 BS 完成信用贷款.

(2)账户安全:每个用户节点都有一个与其资源账户对应的钱包,并且只有使用相应的钥匙和数字证书才能从钱包中获取资源货币.

(3)交易认证:所有交易数据必须经过授权 BSs 的公开审核和验证. 在交易数据构造成区块之前,授权 BSs 会找到并纠正错误的交易数据.

(4)数据不可伪造性:原始数据的相关信息是使用对应用户节点的密钥进行加密. 攻击者无法在联盟区块链中伪造任何经过审计和存储的数据[14].

(5)没有双重支付:资源货币依靠数字签名来证明所有权,同时借助交易记录的公开访问,防止双重支付的发生.

5.2 数值结果分析

在基于信用贷款的支付仿真场景中设置 100 个贷款用户,信用等级 n 设置为 1,2,…,35. 第 n 个信用等级对应的信用等级因子为:$\phi_i=1-(n-1)/N$. 贷款用户根据信用等级概率分布[15]进行分配,将这些贷款用户分

为5组,分别从5家信用银行申请贷款. 每个资源货币有限的信用银行只向20个贷款用户提供贷款. 其他的参数如下表所示:

表1　仿真参数设置

参数	设置值的范围
预定义因子 e_i	[100,140]
预定义因子 k_i	[0.04,0.05]
预定义因子 t_i	(0,1]
预定义因子κ_i	3.5
预定义因子 w	10000
还款缓冲区内偿还贷款概率 g_i	(0,1]
信用等级因子ϕ_i	(0,1]
贷款的单元成本 c_i	[0.1,0.2]

图4显示了随机选择的信用银行经济利益和贷款用户的最优贷款额之间的收敛演变. 随着迭代次数的增加,信用银行的经济效益逐渐上升. 在经过19次迭代后,经济效益和最优贷款额分别快速收敛到稳定值.

图5(*a*)显示了信用等级因子ϕ_i对信用银行平均经济效益的影响. 图5(*b*)显示了信用等级因子ϕ_i对信用银行平均经济效益增长效率的影响. 由图5(*a*)可知信用银行的平均经济效益随着ϕ_i的增加而减少. 因为信用等级较高的贷款用户更有可能及时偿还贷款,从而减少信用银行的罚款,降低了银行的经济效益. 由图5(*b*)可知信用银行的经济效益增长效率随着贷款利率的增加而减少,并逐渐收敛. 这是因为贷款利率的增加会导致贷款金额的减少,降低了信用银行的经济效益增长效率.

图6(*a*)显示了还款缓冲区内偿还贷款概率 g_i对贷款用户平均经济效益的影响. 由图6(*a*)可知,贷款用户的经济利益随着贷款用户的偿还能力 g_i的增加而增加. 图6(*b*)显示了还款缓冲区内偿还贷款概率 g_i对贷款用户平均经济效益增长效率的影响. 由图6(*b*)可知,随着贷款利率的增长,贷款用户经济效益会出现很小程度的降低,但是影响不大.

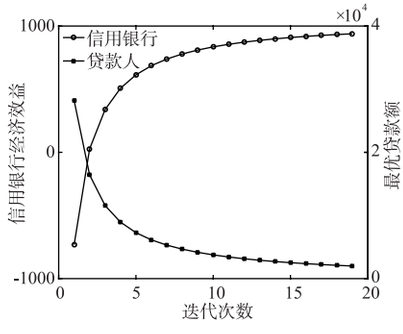

图4　信用银行经济效益与最优贷款额的收敛比较

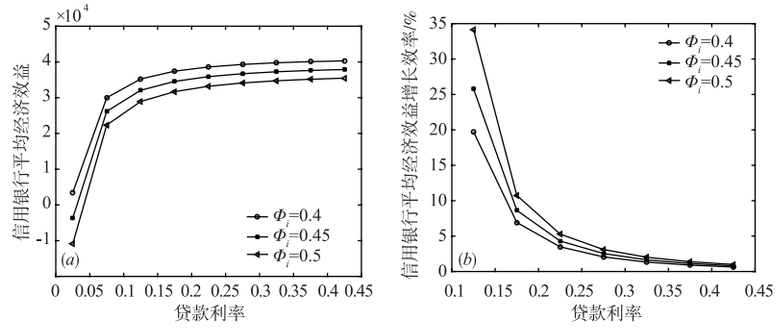

图5　信用等级因子Φ_i与信用银行平均经济效益的关系

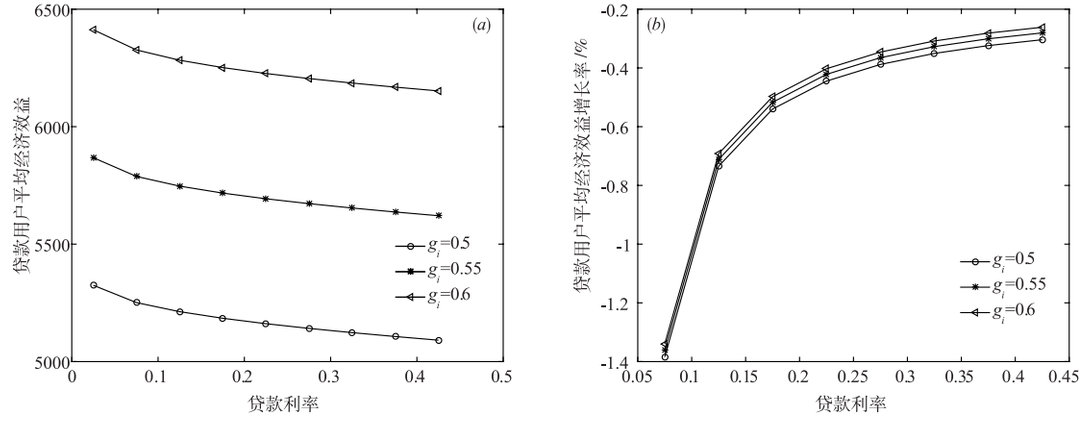

图6　还款缓冲区内偿还贷款概率g_i与贷款用户平均经济效益的关系

6　结论

在SCMA mMTC系统中基于联盟区块链的无线电资源交易模型中,本文提出了一种基于信用的支付方案,支持交易双方之间通过基于信用的支付方案进行频繁的资源交易,提升空闲频谱的利用率. 同时使用

Stackelberg 博弈进行资源货币贷款的最优定价策略,以最大化信用银行的经济效益. 在文章最后,分别对基于信用贷款的支付方案进行安全性和性能分析,以评估所提出基于信用的支付方案. 安全性分析表明,所提出的无线电资源交易模型实现了安全的资源交易,数值结果表明基于信用贷款的支付方案是有效的.

参考文献

[1] Zheng K, Ou S, Alonso-Zarate J, et al. Challenges of massive access in highly dense lte-advanced networks with machine-to-machine communications[J]. IEEE Wireless Communications, 2014, 21(3): 12 – 18.

[2] Nikopour H, Baligh H. Sparse code multiple access[A]. Personal Indoor and Mobile Radio Communications[C]. London: IEEE, 2013, 332 – 336.

[3] Haykin S. Cognitive radio: brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(2): 201 – 220.

[4] Kang J, YU R, Huang S, et al. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicle using consortium blockchains[J]. IEEE Transactions on Industrial Informatics, 2017, 13(6): 3154 – 3164.

[5] Niyato D, Hossain E. Spectrum trading in cognitive radio networks: a market-equilibrium-based approach[J]. IEEE Wireless Communications, 2008, 15(6): 71 – 80.

[6] Aitzhan Z N, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840 – 852.

[7] Yu D, He S, Huang Y, et al. A fast parallel matrix inversion algorithm based on heterogeneous multicore architectures [A]. 2015 IEEE Global Conference on Signal and Information Processing[C]. 2015. 903 – 907.

[8] Castro M, Liskov B. Practical Byzantinefault tolerance [A]. Symposium on Operating Systems Design and Implementation[C]. USENIX Association, 1999. 173 – 186.

[9] Li Z, Kang J, Yu R, et al. Consortium blockchain for secure energy trading in industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3690 – 3700.

[10] Wang J, et al. Perverse nudges: Minimum payments and debt paydown in consumer credit cards[A]. Society for Economic Dynamics [C]. TORONTO: Penn Wharton Public Policy Initiative, 2014. Book 25.

[11] Tushar W, Chai B, Yuen C, et al. Energy management for a user interactive smart community: A Stackelberg game approach[A]. IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA)[C]. Kuala: IEEE, 2014. 709 – 714.

[12] Maharjan S, Zhu Q, Zhang Y, et al. Dependable demand response management in the smart grid: a stackelberg game approach[J]. IEEE Transactions on Smart Grid, 2018, 4(1): 120 – 132.

[13] Su Z, Xu Q, Hui Y, et al. A game theoretic approach to parked vehicle assisted content delivery in vehicular Ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(7): 6461 – 6474.

[14] Linn L A, et al, Blockchain for health data and its potential use in health it and health care related research[A]. ONC/NIST Use of Blockchain for Healthcare and Research Workshop [C]. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

[15] Lending Club Loan Data [EB/OL], Available: https://www.kaggle.com/wendykan/lending-club-loan-data. 2016.

作者简介

孙 君(通信作者) 女,1980 年生,2008 年毕业于山东大学获得博士学位,现为南京邮电大学教师,研究方向:无线网络,无线资源管理和物联网.

E-mail: sunjun@njupt.edu.cn

熊 关 男,1994 年生,现在南京邮电大学攻读硕士学位,主要从事物联网技术相关研究.

E-mail: 1216012030@njupt.edu.cn