一种改进的区块链共识机制的研究与实现

张 永,李晓辉
(华北计算技术研究所 北京 100083)

摘要: 基于在区块链系统中利用共识机制使节点快速、安全的达到数据一致性的目的,文中提出了一种改进的股权授权证明(Delegated Proof Of Stake,DPOS)共识机制,采用基于信用奖惩和投票结果选择优化两个核心方案实现快速剔除异常节点以提高系统安全性。通过搭建分布式网络进行实验,对比分析了机制改进前后的实验结果,验证了在基于信用的奖惩机制下,异常节点再次成为代理节点的概率由84%降低到了5%;并且异常节点被踢出代理所需投票轮数由2.5轮降低到了1.1轮,从而降低了异常节点对系统的影响。

关键词: 区块链; 共识机制; DPOS; 信用; 奖惩机制
中图分类号: TN91 **文献标识码:** A **文章编号:** 1674-6236(2018)01-0038-05

The research and implementation of an improved blockchain's consensus mechanism

ZHANG Yong, LI Xiao-hui
(*North China Institute of Computing Technology*, *Beijing* 100083, *China*)

Abstract: Based on the purpose of using the consensus mechanism to make the nodes reach the consistency of data quickly and safely in the blockchain system. This paper proposes an improved DPOS. It used the reward and punishment mechanism based on credit and optimized voting result to achieve rapid removal of abnormal nodes to improve system security. Through the construction of a distributed network to experiment, this study compared and analyzed the experimental results before and after the improvement of DPOS. It proved that the probability of abnormal nodes become agent again is reduced from 84% to 5% under the credit-based reward and punishment mechanism. And the rounds of abnormal nodes were removed is reduced from 2.5 to 1.1, thus it reduced the impact of abnormal nodes on the system.

Key words: blockchain; consensus mechanism; DPOS; credit; rewards and punishment mechanism

区块链作为比特币的底层技术,是一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案[1-2]。共识机制是区块链的核心,解决了如何在一个缺乏信任、完全自由开放的网络中达成共识的问题[3]。

自文献[1]提出比特币以来,业界对区块链的研究如火如荼,涉及到金融、物联网、版权保护和农业等多个领域[4-8]。为了促进区块链的发展,专家学者相继提出了Bitcoin-NG[9]、权益证明(Proof Of Stake,POS)、DPOS等在内的多种共识机制[2]。这些共识机制在资源消耗、安全性或共识时间等方面各有侧重[10-11]。如在DPOS机制中,节点通过投票选取代理节点的方式产生区块,达成数据的共识可以达到秒级,但网络节点会出现投票不积极的情况,而且如果代理节点中出现了恶意节点,系统不能及时的剔除,导致系统的安全性降低等问题[3]。

文中重点针对DPOS中存在的问题进行改进[3],提出了一种改进的DPOS共识机制。在节点投票和代理节点的选择条件方面做了优化。通过信用奖惩和反对票机制,能够实现在同等条件下,提高网络节点投票的积极性,并且可以通过快速剔除恶意代理节点以提高系统的安全性。

1 区块链共识机制分析

共识是指相互独立的多个参与方对某一问题达

收稿日期: 2017-05-11 **稿件编号:** 201705068
基金项目: 中国电科主导类创新基金项目(JJ120102)
作者简介: 张 永(1992—),男,河北邯郸人,硕士研究生。研究方向:物联网体系架构和区块链技术。

成一致的结果。区块链中的共识是指在开放的分布式网络中各节点对某一区块达成的一致性，是区块链的核心。共识机制主要研究的是区块产生的记账权分配问题和区块产生后的校验问题。目前，围绕共识机制的研究内容，区块链系统存在的共识算法主要有POW、POS、POL和DPOS等。

1.1 POW

2008年，文献《Bitcoin: A Peer-to-Peer Electronic Cash System》中提出了POW（Proof-Of-Work）即工作量证明共识机制，并成功应用在比特币中。该机制是通过各节点进行哈希运算争取区块记账权。区块产生后，向全网进行广播，供其他节点进行验证[12-13]。其优点是可以解决在完全开放、自由的网络中的数据一致性问题。但是区块的产生需要消耗大量的算力和其他资源，并且数据达成一致性时间较长，通常在10分钟以上，难以满足普遍的业务需求[14]。

1.2 POS

针对POW的资源浪费、共识时间较长等问题，文献[15]提出POS共识机制。POS的主要思想是节点获得区块记账权的难度与节点所持有的代币成反比，代币即节点在系统中持有的权益，持有代币多且时间长的节点，在争取区块记账权时越容易获胜[16]。相比较POW，POS在一定程度上减少了数学运算带来的资源消耗，代币的引入也缩短了达成共识的时间。但是POS依然没有摆脱挖矿的本质，在一些共识时间要求比较高的业务环境中并不适用，没有从根本上解决商业应用的痛点。

1.3 POL

POL（Proof-of-Luck）是文献[16]提出的共识机制，是一种在可信执行环境之上建立的共识机制[17]。该机制在每轮区块的产生过程中，会随机产生一个数字以决定一段时间内的获胜区块。可以提高区块产生的效率，降低资源的消耗。但是可信执行环境是一种芯片级的，对处理器提出了一定的要求，所以对于区块链来说，网络的扩展需要节点有相应的硬件支持。

1.4 DPOS

DPOS是在文献[18]中提出的一种可以实现区块秒级验证的共识机制，能够满足广泛的业务需求。DPOS与POS[19]共识机制的主要区别是区块记账节点的选择方式不同，在DPOS共识机制中，每一个持有代币的节点都是候选节点，各节点通过投票的方式选择若干代理节点，由代理节点按照既定的时间表轮流进行区块的产生和验证。

在该机制下，没有消耗算力的挖矿过程，大幅度缩小了参与区块产生和验证的节点数量，可以达到秒级的共识验证。但是在DPOS中对恶意节点没有及时的响应措施，只是对状态进行标识，并且存在节点投票不积极的现象，导致系统的安全性降低等问题。

2 改进的DPOS共识机制

DPOS共识机制通过节点投票选出代理节点进行区块的产生和确认，可以实现秒级的区块验证，能够适应广泛的业务领域。针对DPOS共识机制投票不积极和恶意代理节点未及时剔除导致的安全性较低等问题，本文定义了节点状态、信用系数等基本概念，并提出了基于信用奖惩的改进DPOS机制。在信用奖惩下，全网节点通过投反对票的方式可以降低异常节点成为代理节点的概率，并且结合结果选择条件的优化，可以加快异常节点被踢出代理节点的速度。下面对这种机制进行详细介绍。

2.1 基本原理

文中首先定义了节点状态、状态变更和信用系数等基本概念；其次提出了基于信用的奖惩方案以激励网络节点积极参与到投票中来；最后对代理节点的得票结果进行了优化，可以结合基于信用的奖惩方案达到对异常节点快速剔除的目的。

2.1.1 节点状态

DPOS机制是通过代理节点进行区块的产生和确认的，为了有效监视代理节点的行为，防止恶意节点持续性地产生无效区块或其他恶意行为，给每个节点添加一个状态标识。本文将节点的状态定义为4种，分别是：

1）GOOD：代表良好状态，表示该代理节点连续产生有效区块次数超过累计值（累计值是一个节点状态变更的常量），并通过其他节点验证；

2）NORMAL：代表正常状态，表示该代理节点产生的区块无无效区块，新生代理节点初始状态为NORMAL；

3）EXCEPTION：代表异常状态，表示该代理节点产生过无效区块，但次数小于累计值；

4）ERROR：代表恶意状态，表示该代理节点多次产生无效区块。

节点状态是评判节点是否为恶意节点的标准。

为让状态为GOOD的节点尽可能的被选为代理节点，也防止状态为EXCEPTION节点被选为代理节点，在节点进行投票时，系统将予以节点状态提示。

2.1.2 状态变更

状态变更是指代理节点的状态变化，主要与代理节点产生区块的数量以及有效性相关。当一个新的节点成为代理节点时，系统默认为其分配NORMAL状态，可正常参与之后的代理节点竞选。当代理节点一直保持良好的区块产生记录，即产生有效区块次数大于累计值时其状态可升级为GOOD，GOOD状态的代理节点在之后的代理节点竞选过程中将会有一定的优势。而当代理节点有产生无效区块的记录时，其状态将成为EXCEPTION，在其后的代理节点竞选时，将处于一定的劣势。若代理节点产生的无效区块超过累计值时，其状态将转变为ERROR状态，为了避免恶意节点持续对系统恶意影响，在一段时间内禁止参与之后的代理节点竞选。代理节点的状态转换可用图1描述。

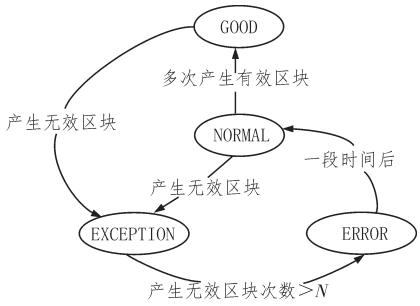

图1 状态转换图

2.1.3 信用系数

信用系数（Credit）是节点加入分布式网络中时系统赋予的一种信用参数，是节点信用程度的一种表现形式。在共识机制中，信用系数将以百分制计数，对于每一个初次接入系统的网络节点，信用系数将被初始化为50。

在不同业务领域的区块链系统中，信用系数可以有不同的含义。当与实际的业务结合起来时，信用系数将被赋予实际的价值，如使用区块链在域名申请解析领域中，通过信用系数可以设定域名的有效期；或者在数字货币领域中，信用系数可以折合成一定的数字货币等。

2.2 基于信用的奖惩方案

基于信用的奖惩方案主要包括两个核心要点，分别为投反对票和奖惩方法，其中投反对票是信用奖励的一个手段。该机制的运行原理可用图2所示流程图表示。

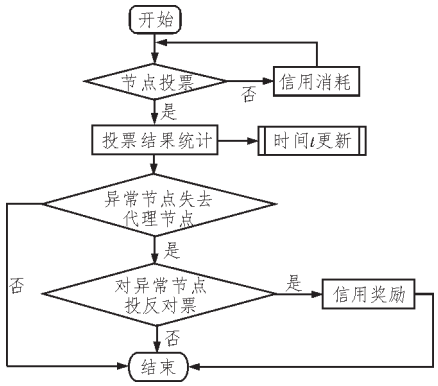

图2 基于信用的奖惩机制流程图安全性

围绕该流程图，下面对该机制进行分模块描述。

2.2.1 投反对票

投反对票是在投票过程中节点可以投反对票的一种方法，目的是为了快速的将异常节点从代理节点中剔除，从而提高系统的安全性投反对票和正常投票的过程相同，节点在投票时，可同时投出反对票和正常票。在共识机制中，采用公钥标识对节点进行唯一表示，公钥的存在使得节点具有匿名性，可以有效避免节点带有目的的投票。

对于状态为EXCEPTION的节点，在投票时系统将予以提示，以期节点能够对其投出反对票，在统计投票结果时可以降低状态为EXCEPTION节点成为代理节点的可能性，从而使系统更加安全。

2.2.2 奖惩方法

信用系数是节点信用的表现形式，基于信用的奖惩方法主要是针对节点而进行的。节点的奖惩机制主要模块构成如图3所示。

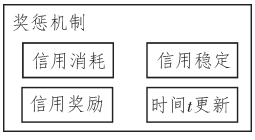

图3 奖惩机制模块图

1）信用消耗

信用消耗是指信用系数会随着时间而降低，在与实际业务结合时，表示的是某种价值的消耗。信用消耗并非一味的降低信用系数，需要遵循一定的规则，满足的公式为：

$$Credit = Credit - \lfloor t/T \rfloor \times M \tag{1}$$

其中，$Credit$表示的是节点的信用系数，t表示节

点从上次投票开始到下次投票的间隔时间，T表示时间常量。当两次投票间隔时间小于T，即$t<T$时，信用系数不发生变化。M表示信用消耗的速度，是一个常量，可结合具体业务对M进行调整。

2）信用稳定和时间重置

当节点两次投票的时间间隔超过T时，信用系数将会降低。相反，信用系数将不发生变化。节点投票成功后会重置时间t，即令t=0，以此鼓励节点参与到投票中来。

3）信用奖励

状态为EXCEPTION的节点是系统不建议成为代理节点的节点。在投票的过程中，每T时间段内，节点只有一个反对票的资格。对投了状态为EXCEPTION节点反对票的节点，若被投反对票的节点未能成为代理节点，系统将给予信用系数奖励，奖励公式为：

$$Credit = Credit + M \tag{2}$$

2.3　优化投票结果统计方案

投票结果统计是竞选代理节点的最后一个过程，合理的计票方式将有助于提升系统的安全性。系统为节点的属性维持着一张动态更新的属性表，如表1所示。

表1　节点属性表

PublicKey	StateType	Credit	Votes	NegativeVotes

该表存储着每一个节点的状态信息、信用系数、得票数以及反对票数。通过该表对结果进行统计，统计公式如下所示：

$$result = A \times Credit + B \times Votes - C \times NegativeVotes \tag{3}$$

其中A是网络中所有节点数量和代理节点数量相关的值，可根据系统的业务以及系统安全性的特征设定A的值。B、C是常量，且满足$B+C=1$，通常B和C取值为0.5。

通过该公式的计算，对于信用系数较低的节点，一般需要获取更多的投票才能成为代理节点。对于状态EXCEPTION节点来说，在信用机制的激励下，成为代理节点的概率将显著降低，并且可以缩短异常节点被踢出代理的时间。

3　实验及分析

文中通过搭建原型系统，对比机制改进前后的运行结果，验证改进后的共识机制是否能够有效降低状态为EXCEPTION的节点（下面使用E节点代替）获取代理节点身份的概率。

3.1　第二轮投票结果验证

本次原型系统搭建建立在一个拥有15个节点的分布式网络上，选举代理节点的数量为3个。投票结果统计公式中常量的取值为：A=1，B=0.5，C=0.5；信用奖惩机制信用消耗的常量取值为：M = 1。

经过一轮投票后，投票结果如图4所示。

在图4中，前3个节点根据投票结果统计公式计算成为代理节点。假设公钥标识为“1f5ccb86225915e276bacce2173dbfb93ce5ffc30731ecd3f71155d2”节点的状态改变为EXCEPTION。

PublicKey	StateType	Credit	Votes	NegativeVotes
afde8d86225915e276bacce2173dbfb93ce5ffc307369da2f326abe5	NORMAL	50	11	0
539f1afbf30ed0aed2bbda53bbc3ca248591b69d85182c80bb81de1a	EXCEPTION	50	8	0
1f5ccb86225915e276bacce2173dbfb93ce5ffc30731ecd3f71155d2	NORMAL	50	5	0
37c6532b0e9372c80a777d8fcca59216bc0bf475e6bdc6f1d48544df	NORMAL	50	4	0
00c15595a96e02238b5a5b8bf43ffc6ddb2b8136185dc8ef8bf0d726	NORMAL	50	2	0
0ce5ce5ea188591cb92f0e627cbefe0c5eeb1f99e78494f3821a45b2	NORMAL	50	0	0
8fcc02160b7fea61de715b4c2fb65746a44dee1e3319a6b64bcb7871	NORMAL	50	0	0
05a455718a2365d6ca1d61d9953445bf38346d6eb370a65894a5fd7f	NORMAL	50	0	0
51b814ae425074a661c2e435e97bcb52291db44c8337fc832b320fc9	NORMAL	50	0	0
ea8b540e10fd49bf23b91ebf4fda26c77a063e0880da9a50a37c7d1b	NORMAL	50	0	0
670edc324b757524ae38a117c83a2c4a5e5aebf14a6989296a92f6d7	NORMAL	50	0	0
9dfedb3f63a62d8c7dba81f00f48dc6c8b1da414f19b0dcb78d6edf8	NORMAL	50	0	0
dda1623c26879f23271244963786026ef927d6fffd95b1e1dcc20cf4	NORMAL	50	0	0
150d62f2f4bcf78671bb8a4e5388ca6262c825739e0c164f005ffbe7	NORMAL	50	0	0
1c8bc13cc7588cae410d662332b3496f31b45174d79dbf451091792a	NORMAL	50	0	0

图4　投票结果

在接下来的实验中，以此次结果为基础进行第二轮投票，实验重点对比分析了DPOS共识机制改进前后第二轮的投票结果，并进行了50次重复实验。根据实验结果对比，绘制出异常节点在第二轮投票结束后的票数排名对比折线图，如图5所示。

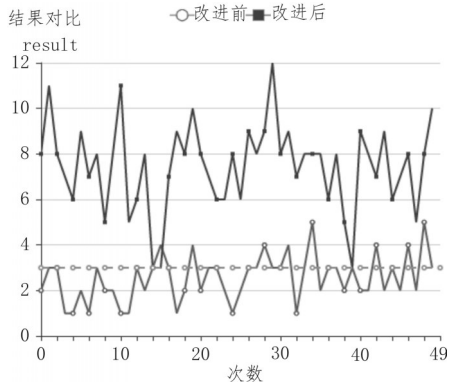

图5　DPOS改进前后结果对比

图5显示，改进后相比于改进前，E节点票数排名明显靠后。并且改进前，E节点在第二轮获得代理节点身份的次数为42次，占总数的84%，而改进后只有3次，占总次数不到5%。该实验表明，E节点成为代理节点的概率显著降低。

3.2　E节点失去代理投票轮数验证

在上述实验的基础上，本次实验主要验证的是DPOS机制改进前后E节点失去代理身份所需要的平均投票轮数是否发生变化。

实验内容是各节点进行多轮投票，直到E节点被踢出代理，然后统计投票轮数。为保证结果的准确性，分别对机制改进前和改进后进行50次重复实验，E节点被踢出代理时投票轮数统计结果如图6所示。

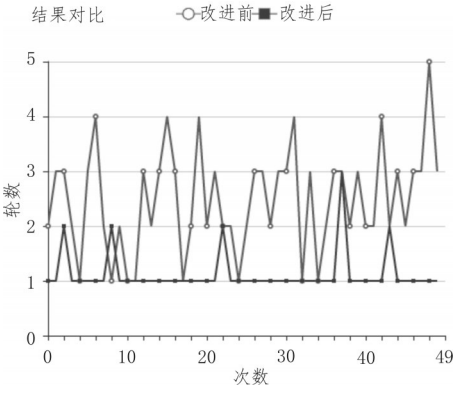

图6　E节点被踢出代理投票轮数对比

对机制改进前后对比实验结果求平均数，求得机制改进前E节点被踢出代理平均需要2.5轮，机制改进后平均需要1.1轮。

由以上实验可以看出，改进的DPOS共识机制，能够使异常节点获取代理节点身份的概率显著降低，并且缩短了异常代理节点被踢出代理的时间，由改进前的需要2.5轮投票降低到了需要1.1轮投票。从而弱化了异常节点对系统的影响，增强了系统的安全性。

4　结束语

区块链是近年来研究的热点，多个行业在使用区块链技术进行业务创新[2]。然而一种共识机制不能够满足所有的业务，不同的业务场景下使用区块链技术所采用的共识机制也不相同，文中对共识机制的研究与改进，解决了DPOS共识机制中存在的对异常节点不能及时剔除等问题，提供了一种共识机制的改进思路，并且通过实验验证了改进后的共识机制的可行性和可用性。改进的DPOS共识机制扩展了能够与区块链技术相结合的业务范围，为下一步区块链的研究提供了方向与基础。

参考文献：

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.

[2] Zheng Z, Xie S, Dai H N, et al. Blockchain Challenges and Opportunities: A Survey[J]. International Journal of Web and Grid Services, 2017.

[3] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J]. 网络与信息安全学报，2016(11):11-20.

[4] 洪涛. 区块链在我国农产品电商领域的应用研究[J]. 中国市场，2016(39):65-68.

[5] 吴健，高力，朱静宁. 基于区块链技术的数字版权保护[J]. 广播电视信息，2016(7):60-62.

[6] 黄峤濛. 区块链携手物联网——打造链上世界[J]. 金卡工程，2016(10):71-73.

[7] 唐文剑，吕雯.区块链将如何重新定义世界[M].北京:机械工业出版社，2016.

[8] 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书[R]. (2016-10-18)[2017-03-10].http://8btc.com/doc-view-985.html.

[9] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: a scalable blockchain protocol[J]. Cryptography and Security, 2015:45-59.

[10]谭磊，陈刚.区块链2.0[M].北京:电子工业出版社，2016.

[11]朱岩，甘国华，邓迪，等. 区块链关键技术中的安全性研究[J]. 信息安全研究，2016,2(12):1090-1097.

（下转第47页）

[2] 徐鑫.入侵防御系统攻击特征库的建立方法研究[D].成都:电子科技大学,2011.
[3] 朱红萍，巩青歌，雷战波. 基于遗传算法的入侵检测特征选择[J]. 计算机应用研究，2012,29(4):1417-1419.
[4] 杨雅辉,黄海珍,沈晴霓,等. 基于增量式GHSOM神经网络模型的入侵检测研究[J]. 计算机学报，2014(5):1216-1224.
[5] 高妮,高岭,贺毅岳,等. 基于深度信念网络的入侵检测模型[J]. 东南大学学报(英文版)，2015(3):339-346.
[6] 王声柱，李永忠. 基于深度学习和半监督学习的入侵检测算法[J]. 信息技术，2017(1):101-104.
[7] 肖立中，刘云翔，陈丽琼. 基于改进粒子群的加速K均值算法在入侵检测中的研究[J]. 系统仿真学报，2014，26(8):1652-1657.
[8] 谭爱平，陈浩，吴伯桥. 基于SVM的网络入侵检测集成学习算法[J]. 计算机科学，2014，41(2):197-200.
[9] 武小年,彭小金,杨宇洋,等. 入侵检测中基于SVM的两级特征选择方法[J]. 通信学报，2015，36(4):19-26.
[10]刘铭，黄凡玲，傅彦铭,等. 改进的人工蜂群优化支持向量机算法在入侵检测中的应用[J]. 计算机应用与软件，2017(1):230-235.
[11]江颉，王卓芳，陈铁明,等. 自适应AP聚类算法及其在入侵检测中的应用[J]. 通信学报，2015，36(11):118-126.
[12]康松林，刘乐，刘楚楚,等. 多层极限学习机在入侵检测中的应用[J]. 计算机应用，2015，35(9):2513-2518.
[13]杜晔，张亚丹，黎妹红,等. 基于改进FastICA算法的入侵检测样本数据优化方法[J]. 通信学报，2016，37(1):42-48.
[14]魏琴芳，成勇，胡向东. 基于信息熵的无线传感网入侵检测遗传算法[J]. 重庆邮电大学学报:自然科学版，2016(1):107-112.
[15]刘珊珊，谢晓尧，徐洋,等. 基于PCA的PSO-BP入侵检测研究[J]. 计算机应用研究，2016，33(9):2795-2798.
[16]吴丽云，李生林，甘旭升,等. 基于PLS特征提取的网络异常入侵检测CVM模型[J]. 控制与决策，2017，32(4):755-758.
[17]许学添.基于模糊约束的网络入侵检测方法[J].西安工程大学学报,2016,30(5):627-632.
[18]张耀元,郭淑明,汪小雨.基于入侵检测技术的MANET安全研究[J].电子科技,2016,30(5):627-632.

(上接第42页)

[12]袁勇,王飞跃. 区块链技术发展现状与展望[J]. Acta Automatica Sinica，2016,42(4):481-494.
[13]梁斌. 从“比特币挖矿”看区块链技术的共识机制[J]. 中国金融电脑，2016(9):45-46.
[14]Decker C，Wattenhofer R. Information propagation in the Bitcoin network[C]// IEEE Thirteenth International Conference on Peer-To-Peer Computing. IEEE，2013:1-10.
[15]Larimer D.Transactions as proof-of-stake[EB/OL]. http://7fvhfe.com1.z0.glb.clouddn.com/@/wpcontent/uploads/2014/01/Transactions As Proof Of Stake10.pdf . 2013.
[16]King S，Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper，August，2012:19.
[17]Milutinovic M，He W，Wu H，et al. Proof of Luck: an Efficient Blockchain Consensus Protocol[C]// Proceedings of the 1st Workshop on System Software for Trusted Execution. ACM，2016: 2.
[18]Larimer D.Delegated proof-of-stake white paper[EB/OL].http://www.bts.hk/dpos-baipishu.html.2014.
[19]刘秋连.O2M全渠道视角下零售企业会员营销模式的构建[J].西安工程大学学报,2016(5):669-674.