基于量子隐形传态的无线通信网络身份认证方案*

张沛 周小清† 李智伟

(吉首大学物理与机电工程学院, 吉首 416000)

(2014 年 2 月 14 日收到; 2014 年 3 月 19 日收到修改稿)

提出了有中心的结构化量子通信网络概念, 并在经典认证基础之上, 结合量子隐形传态技术实现了无线通信网络的身份认证. 此认证方案通过对无线局域网的认证进行探讨进而推广至整个无线通信网络中. 在无线局域网中, 在已获得 SK 与 EPR 对的前提下, STA 与 AP 两端通过量子信道进行信息传输, 然后 AP 对手中的量子态进行幺正变换后将得到的信息与原先的备份信息进行保真度计算, 从而判定是否认证成功.

关键词: 量子通信, 量子隐形传态, 身份认证, 有中心结构化网络

PACS: 03.67.Dd, 42.50.Ex, 89.70.–a **DOI:** 10.7498/aps.63.130301

1 引 言

量子通信为一门新兴的交叉学科, 是信息论与量子论相结合的产物, 由于其具有高效率与绝对安全等特点, 在过去的 20 年中, 量子通信技术得到了飞速的发展. 根据传输信息的不同, 量子通信可分为两类: 传输经典信息的量子密钥分配和传输量子信息的量子隐形传态. 前者主要用于量子密钥的传送, 后者主要用于未知量子态的传送. 量子隐形传态作为一种经典通信无法比拟的瞬时量子信息传输技术, 自从 1993 年被 Bennett 等提出 [1], 便引起了各国科学家的广泛关注. 1997 年 Bouwmeester 小组利用纠缠光子对作为量子信道实现了量子隐形传态 [2], 从实验方面证明了量子隐形传态的客观存在性; 2000 年 Guo 小组提出了一种隐形传态方案 [3], 该方案理论上实现了多个粒子的量子隐形传态; 2004 年 Gobby 等实现了在 122 km 光纤中的量子通信实验 [4]; 随后, Pan 小组在 2005 年与 2012 年分别实现了 13 km 的双向量子纠缠分发与百 km 级的自由空间量子隐形传态和纠缠分发 [5,6]; 2013 年 Peng 等提出了新的方案, 此方案通过不同的量子信道实现了多粒子任意态的量子隐形传送 [7]. 此外, 在量子通信网络的结构与协议方面, 国内外科学家也取得了丰硕的研究成果. 周南润小组利用量子力学中纠缠态的非定域关联性提出了数据链路层的相关协议 [8−10], 从而有效地提高了数据链路层的最大吞吐量和信道利用率; Dupuis 小组设计了量子广播信道协议 [11]; Yu 小组提出了无线分布式量子通信网络的概念并解决了该网络内的信息传输问题 [12]; 周小清小组先后对量子隐形传态网络及网络通信协议进行了研究, 提出了相关的方案与协议 [13,14].

尽管各国科学家进行了大量工作, 取得了丰硕成果, 但关于量子通信网络身份认证方面的研究仍然较少. 虽然, Zhou 小组、温晓军小组与 Zeng 小组针对此方向进行了一系列工作, 分别提出了基于量子隐形传态的跨中心量子身份认证方案、分布式量子通信网络中的身份认证方案与基于偏振调制的量子认证方案 [15−17], 但该方向仍有广阔的研究空间, 因此本文将量子隐形传态技术与无线通信网络相结合, 提出了基于量子隐形传态的无线通信网络身份认证方案.

* 湖南省自然科学基金 (批准号: 11JJ3003, 13JJ3092) 和湖南省科技计划 (批准号: 2010FJ3081) 资助的课题.

† 通讯作者. E-mail: zhouxq_jd@163.com

2 量子隐形传态原理

量子隐形传态是利用量子纠缠对(EPR对)所实现的远程关联, 即发送者分别通过量子信道与经典信道将量子信息与经典信息发送给接收者. 接收者在收到两种信息的前提下, 可得到原量子态的复制品. 其过程如下:

制备n个EPR对:

$$|\psi^-\rangle_{23}^1=\frac{1}{\sqrt{2}}\left(|01\rangle_{23}^1-|10\rangle_{23}^1\right), \tag{1}$$

$$|\psi^-\rangle_{23}^2=\frac{1}{\sqrt{2}}\left(|01\rangle_{23}^2-|10\rangle_{23}^2\right), \tag{2}$$

$$|\psi^-\rangle_{23}^3=\frac{1}{\sqrt{2}}\left(|01\rangle_{23}^3-|10\rangle_{23}^3\right), \tag{3}$$

$$\cdots$$

$$|\psi^-\rangle_{23}^n=\frac{1}{\sqrt{2}}\left(|01\rangle_{23}^n-|10\rangle_{23}^n\right), \tag{4}$$

其中粒子2掌握在发送方手中, 粒子3处于接收方手中, 发送方所要传达的信息体现在以下的量子比特流中:

$$|\psi\rangle_1^1=a_1|0\rangle_1^1+b_1|1\rangle_1^1, \tag{5}$$

$$|\psi\rangle_1^2=a_2|0\rangle_1^2+b_2|1\rangle_1^2, \tag{6}$$

$$|\psi\rangle_1^3=a_3|0\rangle_1^3+b_3|1\rangle_1^3, \tag{7}$$

$$\cdots$$

$$|\psi\rangle_1^n=a_n|0\rangle_1^n+b_n|1\rangle_1^n. \tag{8}$$

粒子1, 2, 3组成的系统量子态为

$$\begin{aligned}&|\psi\rangle_{123}^n\\&=|\psi\rangle_1^n\otimes|\psi^-\rangle_{23}^n\\&=(a_n|0\rangle_1^n+b_n|1\rangle_1^n)\otimes\frac{1}{\sqrt{2}}(|01\rangle_{23}^n-|10\rangle_{23}^n).\end{aligned} \tag{9}$$

由于发送方处持有的粒子为(1, 2)且所做的测量为判断粒子1和粒子2处于哪个Bell纠缠态. 因此我们将上述函数按四个Bell基态展开:

$$\begin{aligned}|\psi\rangle_{123}^{\rm n}=&-\frac{1}{2}\left[|\psi^-\rangle_{12}^{\rm n}\left(a_{\rm n}|0\rangle_3^{\rm n}+b_{\rm n}|1\rangle_3^{\rm n}\right)\right]\\&-\frac{1}{2}\left[|\psi^+\rangle_{12}^n(a_n|0\rangle_3^n-b_n|1\rangle_3^n)\right]\\&+\frac{1}{2}\left[|\Phi^-\rangle_{12}^n(a_n|1\rangle_3^n+b_n|0\rangle_3^n)\right]\\&+\frac{1}{2}\left[|\Phi^+\rangle_{12}^{\rm n}\left(a_{\rm n}|1\rangle_3^{\rm n}-b_{\rm n}|0\rangle_3^{\rm n}\right)\right].\end{aligned} \tag{10}$$

通过经典信道, 发送方将测量结果传送给接收方. 随后, 接收方根据发送方的测量结果, 对粒子3进行相应的幺正变换便可使粒子3处在发送方的未知量子态$|\psi\rangle_1^n$上. 粒子3所处的量子态及相应的幺正变换由表1列出.

表1 粒子3所处的量子态及相应的幺正变换

发送方的测量结果	粒子3的量子态	接收方的幺正变换
$|\psi^-\rangle_{12}^n$	$-(a_n|0\rangle_3^n+b_n|1\rangle_3^n)$	$-\mathrm{I}$
$|\psi^+\rangle_{12}^n$	$-(a_n|0\rangle_3^n-b_n|1\rangle_3^n)$	$-\sigma_z$
$|\Phi^-\rangle_{12}^n$	$(a_n|1\rangle_3^n+b_n|0\rangle_3^n)$	σ_x
$|\Phi^+\rangle_{12}^n$	$(a_n|1\rangle_3^n-b_n|0\rangle_3^n)$	$i\sigma_y$

3 有中心的结构化量子通信网络模型

无线局域网[18]的拓扑结构分为两种: 一种为自组织无线网络(Ad-hoc), 另一种为有中心的结构化无线网络(Infrastructure), 如今大多数的蜂窝移动通信网络都属于后者. 有中心的结构化量子通信网络定义如下: 此网络包含一个无线接入点(Access Point, AP)及若干节点(各个节点皆为具有无线通信功能的量子移动设备). 无线接入点与节点间存在量子信道(两者之间拥有EPR对)与经典信道, 量子信道进行信息的传输, 无线信道作为经典信道起辅助作用.

与无线自组织网络相比, 有中心的结构化网络通常需要一个无线接入点作为中心点, 所有节点对网络的访问均由此中心点控制. 由于中心点的存在, 因此, 当网络业务量增大时, 网络的时延性与吞吐性恶化并不剧烈. 此外, 由于每个节点只需在中心点覆盖范围之内便可以与其他节点进行通信, 因此中心点的布局受环境的限制很小[19]. 虽然有中心的结构化网络有众多优点, 但安全问题仍是其不可忽略的重要问题. 因此, 通过将量子隐形传态与经典网络相结合的方式, 形成新的有中心的结构化量子通信网络, 从而运用量子隐形传态技术解决无线局域网的安全问题.

图1中, ⚡ 表示无线信道, 虚线表示量子信道, 实线代表有线信道. 该网络采用了总线结构, 以AP为中心的局域网采用了星型拓扑结构, AP以有线的方式接入互联网中, 通过光纤与各个固定主机进行通信, 通过量子信道和无线信道与各个移动主机进行通信. 模型中单个移动主机的移动, 加入和退出只影响一个设备, 并不影响全网. 此有中心的结构化量子通信网络模型有以下特点:

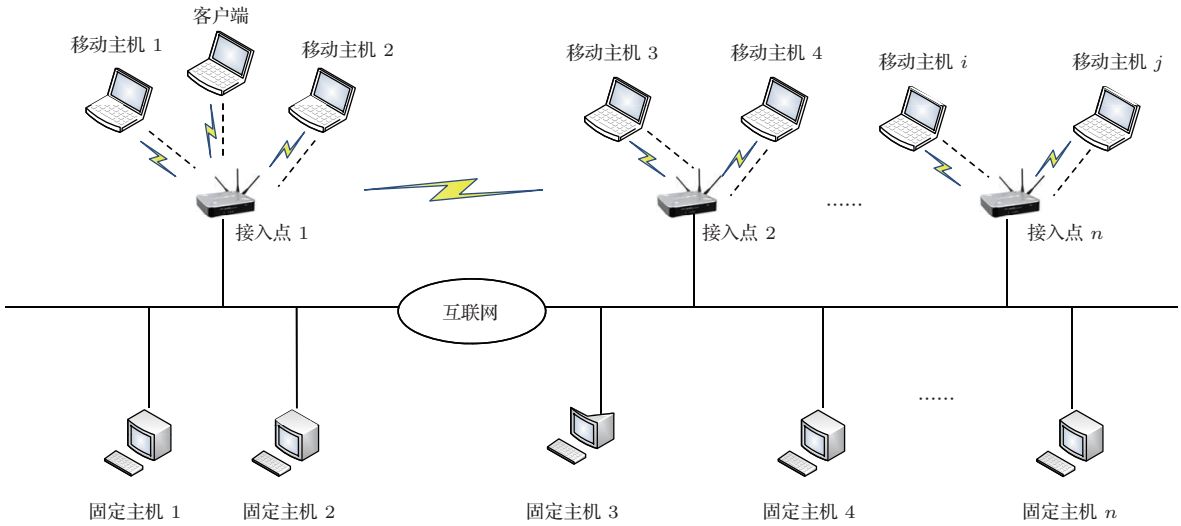

图 1 有中心的结构化量子通信网络模型

1) 网络结构遵循有中心的结构化无线网络结构, 网络中有一个中心点, 相邻之间移动主机不可以直接通信, 各移动主机间的通信必须通过中心点, 发送数据的移动主机首先将数据发送至中心点, 再由中心点将信息发送至目的移动主机;

2) 中心点除了具有桥接功能外, 还负责对各节点的认证、登陆、漫游的管理等;

3) 信息不再通过经典信道传送, 当移动主机与中心点建立起量子信道后, 量子态携带信息通过量子信道进行瞬间传输, 不受障碍物的阻碍, 且与通信实体没有关联.

4 基于量子隐形传态的无线通信网络认证算法

4.1 经典无线局域网的认证

随着无线局域网的发展, 其安全问题也随之产生, 为了应对不断出现的无线局域网安全问题, 新的 WLAN 安全标准 IEEE802.11i 于 2004 年发布. 此协议从认证和加密两方面加强了无线局域网的的安全性, 在加密方面定义了 TKIP, CCMP 和 WRAP 三种加密机理: 在认证方面, 802.11i 协议采用了基于端口的访问控制技术 IEEEE802.1X. 其认证过程如图 2 所示.

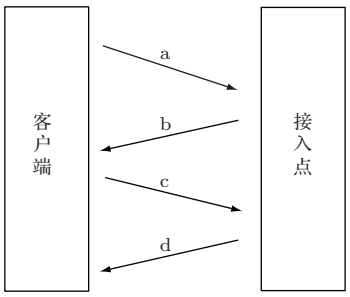

图 2 无线局域网认证过程示意图 (a. 认证请求, b. 认证响应 (含质询), c. 对质询信息的响应, d. 认证成功确认)

4.2 量子无线局域网认证方案

与经典无线局域网相同, 在量子无线局域网中, 如果新的客户端需要加入网络, 必须在得到接入点的许可之后才能加入局域网中. 因此, 在经典无线局域网认证方法的基础之上, 提出了一种无线量子局域网的认证方案. 由于开放系统认证的安全性极低, 本文只讨论双方在共享密钥 (SK) 下的认证. 如下为客户端 (STA) 与接入点 (AP) 的基本认证过程, STA 与 AP 共享 SK, 且在 STA 和 AP 之间已经通过网络服务商共享了 EPR 对.

认证过程及算法:

1) STA 向 AP 发送认证请求, 此认证请求为管理帧, 其量子帧格式为

2	2	6	6	6	2	0-2312	4
Fra-control	Duration	DA	SA	BSSID	Seq-control	Fra-body	FCS

Fra-control为帧控制字段, 描述与控制MAC帧相关信息, 2个量子字节;

Duration为持续时间, 多数情况下用于设定计时器, 2个量子字节;

DA为目的地址, MAC帧的目的地址, 6个量子字节;

SA为来源地址, MAC帧的源地址, 6个量子字节;

BSSID为基本服务集标识, 用于过滤收到的MAC帧, 6个量子字节;

Seq-control为序列控制域, 用来重组帧片段及丢弃重复帧, 2个量子字节;

Fra-body为帧主体, 封装的为上层的数据单元, 长度最多可达2312量子字节;

FCS为校验域, 验证是否有误, 4个量子字节.

2) AP在收到认证请求后, 向STA发回一个质询信息, 此质询信息为长度为128量子字节的质询帧, 其帧格式与i中量子帧格式相同. 在发送质询信息之前, 根据Buzek-Hillery的普适克隆机原理[20,21], AP将作为质询信息的量子帧进行复制, 一份发送给STA, 一份自己保留.

3) 当STA接收到来自AP的质询信息帧后, 通过量子隐形传态将质询信息的量子帧$(|\psi\rangle_1^1, |\psi\rangle_1^2, \cdots, |\psi\rangle_1^n)$发回给AP. STA依次对质询信息和自己拥有的EPR纠缠对进行BELL基测量, 当所有测量都完成后, STA会得到$2n$个比特的经典信息, 用SK加密后发送给AP. 从而对质询信息进行响应.

4) AP用SK对加密过的经典信息解密, 并根据解密后的经典信息, 对自己手中的量子态进行幺正变换, 得到隐形传送过来的质询信息$(|\psi'\rangle_1^1, |\psi'\rangle_1^2, \cdots, |\psi'\rangle_1^n)$. 将收到的信息与发送前的备份进行保真度(Fidelity)的计算, 如若两者完全相同, $F=1$, 则AP发送确认帧告知STA认证成功; 如果$F<1$, 则认证失败, 确认帧格式为

2	2	6	4
Frame control	Duration	Receiver Address	FCS

Frame control为帧控制字段, 2个量子字节;

Duration为持续时间, 多数情况下用于设定计时器, 2个量子字节;

Receiver Address为接收方地址, 6个量子字节;

FCS为校验域, 4个量子字节.

附:

a. 由于在现实通信中, 保真度很难达到1, 因此我们可以通过实验来确定保真度可以容忍的一个范围, 如0.67[22], 若保真度大于0.67, 我们认为通信成功, 可以进行认证; 若低于0.67, 则认为通信失败, 进行重发(可通过量子编码的方法提高保真度, 具体方法可参见文献[23]).

b. 设置一个约定时间t, 如果STA在时间t内未收到认证响应则返回步骤i, 重新发送认证请求重新开始认证过程.

4.3 量子无线通信网络的认证

如图1所示, 在整个量子通信网络中含有多个无线接入点(AP), 这些接入点的有效范围是相互重叠且覆盖整个网络的. 基于此类模式, 整个量子网络就变成了以有线网络为主干的多接入点无线网络. 如若有新的节点欲进入此网络, 其只需向最近的接入点进行认证(认证过程如上一节所示), 如若认证成功, 便可以访问整个网络, 从而完成量子无线通信网络的认证.

5 方案性能分析

在整个认证过程中, 认证请求与质询信息全为量子帧皆由量子信道进行传送, 而经典信道只作为辅助信道进行测量信息的传送, 因此经典信道的负担大大减少. 由于此认证方案中所传输的信息为量子信息, 因此相对于经典的无线通信网络认证方案, 此方案可以传输的信息将更为丰富. 此外, 由于量子隐形传态技术的瞬时性, 信息的传输时间得到了缩短, 通信效率也得到了提高.

在安全性方面, 量子隐形传态分为两个信道, 在经典信道上, 若STA和AP共享的秘钥是通过量子秘钥分发产生, 则量子秘钥分发[24]的保密性便保证了经典信道的安全性, 使得Eve无法获取SK. 因此, 本方案的前提为采用量子秘钥分发共享SK, 从而保证量子隐形传态中经典信道的安全性. 在量子信道上, 允许Eve采用各种窃听和伪造手段进行攻击, 假定Eve是想伪造STA的身份与AP进行身份认证. 即在第3)中, Eve通过各种手段(如“截断\重发”等)获得了128量子字节的质询信息, 且假定Eve与AP间共享有纠缠对. 根据量子力学原理, Eve若对任意一个未知量子态测量, 都会导致量子态的坍塌, 无法得到任何信息. 于是Eve对截取的

各个量子态和共享的纠缠对进行BELL基测量, 冒充STA进行量子隐形传态, 发回质询信息量子帧. 此外, Eve为了获取认证资格, 需将测量后的经典信息通过经典信道发给AP, 若Eve对测量结果的经典信息采用错误的SK加密或者不采用SK加密, AP根据收到的来自Eve的测量信息, 始终无法还原质询信息的量子态, 而导致Eve无法通过认证. 此外, 在通信过程中, 由于受到环境的影响, 保真度很难达到理想状态1. 通过对保真度的分析, 只要其在0.67—1的范围内, 我们便可认为认证成功, 从而保证了认证的正确性. 因此, 该身份认证方案是安全的, 确保了合法用户的身份认证过程.

6 结 论

本文在经典无线局域网认证协议的基础上, 结合量子隐形传态技术, 研究了基于量子隐形传态的无线通信网络的身份认证方案. 即在STA与AP端共享SK和EPR纠缠对的前提下, 将量子帧作为质询信息通过量子信道在两端间进行传输. AP根据解密的经典信息, 对自己手中的量子态进行幺正变换后, 将得到的质询信息与原先的备份信息进行保真度计算, 从而判定是否认证成功. 通过对此方案进行性能分析可以得出, 此方案在通信效率、信息容量、安全性能等各方面均优于经典认证方案.

参考文献

[1] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters W K 1993 *Physical Review Letters* **70** 1895

[2] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H, Zeilinger A 1997 *Nature* **390** 575

[3] Yang C P, Guo G C 2000 *Chin. Phys. Lett.* **17** 162

[4] Gobby C, Yuan Z L, Shields A J 2004 *Applied Physics Letters* **84** 3762

[5] Pan J W, Yang T, Bao X H, Zhang J, Jin X M, Feng F Y, Yang B, Yang J, Zhang Q, Li N, Tian B L, Peng C Z 2005 *Physical Review Letters* **94** 150501

[6] Peng C Z, Pan J W, Yin J, Ren J G , Lu H, Cao Y, Yong H L, Wu Y P, Liu C, Liao S K, Zhou F, Jiang Y, Cai X D, Xu P, Pan G S, Jia J J, Huang Y M, Yin H, Wang J Y, Chen Y A 2012 *Nature* **488** 185

[7] Peng J Y, Mo Z W 2013 *Chin. Phys. B* **22** 050310

[8] Zhou N R, Cheng H L, Liao Q H 2013 *International Journal of Theoretical Physics* **52** 811

[9] Zhou N R, Zeng G H, Gong L, HLiu S Q 2007 *Acta Phys. Sin.* **56** 5066 (in Chinese) [周南润, 曾贵华, 龚黎华, 刘三秋 2007 物理学报 **56** 5066]

[10] Zhou N R, Zeng B Y, Wang L J, Gong L H 2010 *Acta Phys. Sin.* **59** 2193 (in Chinese) [周南润, 曾宾阳, 王立军, 龚黎华 2010 物理学报 **59** 2193]

[11] Dupuis F, Hayden P, Li K 2010 *IEEE Trans. Info. Theory* **56** 2946

[12] Yu X T, Xu J, Zhang Z C 2013 *Chin. Phys. B* **22** 090311

[13] Zhou X Q, Wu Y W 2012 *Acta Phys. Sin.* **61** 170303 (in Chinese) [周小清, 邬云文 2012 物理学报 **61** 170303]

[14] Yang X L, Zhou X Q, Zhao H, Wang P P 2012 *Acta Phys. Sin.* **61** 020303 (in Chinese) [杨小琳, 周小清, 赵晗, 王朋朋 2012 物理学报 **61** 020303]

[15] Zhou N R, Zeng G H, Zeng W J, Zhu F C 2005 *Optics Communications* **254** 380

[16] Wen X J, Liu Y 2005 *Journal of the China Railway Society* **27** 58 (in Chinese) [温晓军, 刘云 2005 铁道学报 **27** 58]

[17] He G Q, Zeng G H 2005 *Chin. Phys.* **14** 541

[18] Liu N A, Li X H 2004 *Wireless Local Area Networks-Principe, Technique and Application* (Xi'an: Xidian University Press) p5 (in Chinese) [刘乃安, 李晓辉 2004 无线局域网: 原理, 技术与应用 (西安: 西安电子科技大学出版社) 第5页]

[19] Niu W, Guo S Z, Wu Z J 2003 *Wireless Local Area Networks* (Beijing: Posts & Telecom Press) p21 (in Chinese) [牛伟, 郭世泽, 吴志军 2003 无线局域网 (北京: 人民邮电出版社) 第21页]

[20] Buzek V, Hillery M 1996 *Phys. Rev. A* **54** 1844

[21] Bruss D, Divincenzo D P, Ekert A, Fuchs C A, Macchiavello C, Smolin J A 1998 *Phys. Rev. A* **57** 2368

[22] Oh S, Lee S C, Lee H W 2002 *Phys. Rev. A* **66** 22316

[23] Chen X, Zhou X Q, Zhao H, Zhang P 2013 *Chinese Journal of Quantum Electronics* **30** 722 (in Chinese)[陈玺, 周小清, 赵晗, 张沛 2013 量子电子学报 **30** 722]

[24] Bennett C H, Brassard G 1984 *International Conference on Computers, Systems, and Signal Processing* Bangalore, India, December 9–12, 1984 p175

Identification scheme based on quantum teleportation for wireless communication networks*

Zhang Pei Zhou Xiao-Qing† Li Zhi-Wei

(*Department of Physics, Mechanical and Electrical Engineering, Jishou University, Jishou 416000, China*)

(Received 14 February 2014; revised manuscript received 19 March 2014)

Abstract

A concept of infrastructure quantum communication network is proposed, and an identification scheme for wireless communication networks is realized by combining classical certification and quantum teleportation.This identification scheme is discussed through the wireless LAN authentication and extended to the entire wireless communication network. In the wireless local area network, the information is transmitted between STA and AP who obtained the SK and EPR pair via quantum channel. Then AP will obtain the information through unitary transformation and calculate the fidelity with the original backup information, so as to determine whether the identification is successful or not.

Keywords: quantum communication, quantum teleportation, identification, infrastructure network

PACS: 03.67.Dd, 42.50.Ex, 89.70.–a **DOI:** 10.7498/aps.63.130301

* Project supported by the Natural Science Foundation of Hunan Province, China (Grant No. 11JJ3003, 13JJ3092), and the Science and Technology Plan of Hunan Province, China (Grant No. 2010FJ3081).

† Corresponding author. E-mail: zhouxq_jd@163.com