

# 网格环境中基于行为的信任模型研究与改进

倪俊敏,解 福,田宏伟

(山东大学 信息科学与工程学院,山东 济南 250014)

**摘 要:**给出了网格环境下信任的定义,对网格环境中基于行为的信任模型进行了研究,并对其进行了改进。改进模型中的信任抉择采取三级受理的方式,按照“先本地、再同域、最后其他域”的顺序逐级地处理交易请求,使得交易处理有条不紊的进行。介绍了域内直接信任值、域内间接信任值、域内信任值、域间直接信任值及域间间接信任值的计算方法,充分考虑了各种情形,使得评价更加客观和合理,提高了交易成功率,从而为访问决策提供有利且合理的依据。

**关键词:**网格;信任模型;信任代理

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1673-629X(2011)12-0036-05

## Research and Improvement of Trust Model Based on Behavior in Grid Environment

NI Jun-min, XIE Fu, TIAN Hong-wei

(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

**Abstract:** Give the definition of trust in grid environment and research on the trust model based on behavior and its improved model. In the trust model, the choice trust uses the three-level accepted way. In accordance with the “first local, then the same domain, and finally the other domain”, it handles the transaction request step by step, making the orderly conduct of transaction processing. Describe the calculation methods direct trust value, indirect trust value and trust value within the same domain, the direct trust value and indirect trust value between domains. It fully considers to all the circumstances plenty and makes the evaluation more objective and reasonable, increases transaction success rate, so as to provide favorable accesses to decision-making and reasonable basis.

**Key words:** grid; trust model; trust agent

## 0 引言

网格是高性能计算和信息服务的战略性基础设施,也是计算机网络与分布式系统研究的前沿问题之一。网格是把分布在广域网上的各类资源整合起来,提供大规模的分布式计算,在动态的、多个单位参与的虚拟组织之间协同资源共享和解决问题。在网格环境中,网格实体之间存在着信任关系,实体间通信时需要进行信任抉择。由于网格环境的动态性和不确定性,当网格实体进行交易时需要知道它们之间的信任关系。在网格环境中,信任研究的实质是:采用合适的方法对各个网格节点参与者间的信任进行度量、评估和推理,为用户提供有效的信任知识表达、逻辑推理和决策支持的自动工具。目前,信任机制研究工作还有很

多问题和困难需要解决,这也迫切地需要改进网格信任机制,以保证网格的安全性。

## 1 研究现状

网格环境中,信任机制通常分为基于实体域行为的信任机制和基于实体域身份的信任机制两类。在基于实体域行为的信任机制中,每个实体根据其他实体提供的行为评价信息及其他信息来计算网格中每个实体的信任值。但当前的信任研究工作还存在着以下的不足之处<sup>[1]</sup>:

(a) 缺乏统一明确的信任定义,缺乏对信任特征的全面概括。

(b) 信任具有主观性和动态性,但目前对网格的信任模型中信任度量和推理机制对这方面的关注不够。

(c) 没有一个较为综合的网格环境下的信任问题的解决方法。

针对网格的特点,文中充分考虑了网格域内节点

收稿日期:2011-04-14;修回日期:2011-07-21

基金项目:国家自然科学基金(90612003)

作者简介:倪俊敏(1985-),女,硕士研究生,研究方向为网格信息安全;解 福,副教授,硕士生导师,研究方向为网格信息安全和网格资源管理。

间和网格域之间的直接信任和推荐信任,给出信任值计算方法,使信任值更加真实地反映实体的客观可信性,为信任抉择提供了更加客观的依据。

## 2 信任

### 2.1 信任的定义

信任是指相信并加以任用,目前,关于信任尚未有一个可以被广泛接受的定义,ITU-T 推荐标准 X.509 规范中给出的定义:实体 A 认定实体 B 将严格地按 A 所期望的那样行动,则 A 信任 B。这里称 A 是信任者,B 是被信任者。从定义可以看出,信任涉及对某种事件、情况的预测、期望和行为。信任是信任者对被信任者的一种态度,是对被信任者的一种预期,相信被信任者的行为能够符合自己的愿望。根据以上分析,文中定义:信任是指根据对某实体过去行为及其他实体对其的推荐信息,而对此实体本身行为的期望。信任在两个实体之间是一对一的关系,但不是对称的,A 信任 B 的程度不一定等同于 B 信任 A 的程度。

### 2.2 信任关系分类

实体之间的信任关系可以分为直接信任和推荐信任两类<sup>[2]</sup>。

直接信任是最简单的信任形式。两个实体之间无须第三方介绍而直接建立起来的信任关系称为直接信任,即直接信任是两个实体通过直接交易获得的信任关系<sup>[3]</sup>。

推荐信任是指两个实体以前没有建立起信任关系,但双方与共同的第三方有信任关系,第三方为两者的可信任性进行了担保,由此建立起来的信任关系,因此推荐信任值是根据第三方实体对交易双方实体的评估而得出的结果。在采纳其他节点提供的推荐信息时,应该考虑该推荐节点提供的推荐信息的可信程度,推荐节点的推荐信任度越高,信任主体对推荐节点推荐行为的信任程度越高,对被推荐节点的信任程度就越高。推荐信任又分为直接推荐信任和间接推荐信任。直接推荐信任即信任主体直接从一个推荐实体得到信任客体的信息,而间接推荐信任需要从多个推荐实体那里得到信任客体的信息。这样,直接推荐信任和间接推荐信任相结合的方式为信任主体对信任客体的评价更为客观。

## 3 信任模型

### 3.1 信任模型

信任模型,是建立信任关系和验证证书时寻找和遍历信任路径的模型。建立信任模型所需要做的工作是收集、分析各个实体的信任信息,并在此基础上给出信任值的计算方法。

建立合理的信任机制就是为了找到符合信任主体服务请求且可信任的信任客体。信任值作为实体间信任关系的度量依据,信任主体根据其来判断信任客体的行为并做出决策,即与之交易或拒绝与之交易。在合理的信任机制下,信任主体与信任客体发生可信任的交易,提高交易成功率,降低交易失败的风险,减少损失。

基于行为的信任模型的设计思想<sup>[4]</sup>是:将网格划分成若干个自治域,节点间信任关系分为域内信任关系和域间信任关系,采用不同的策略来分别处理域内信任关系和域间信任关系。

其典型的实施策略简要叙述如下:

(1) 域内信任关系基于同域节点间的交易。

网格域中的每个节点都存储直接信任值表和间接信任值表这两张表,在信任客体提交交易请求之后,信任主体先查询本地存储的直接信任值表,若表中存在信任客体的直接信任值,信任主体就直接根据该直接信任值来进行抉择;若不存在该节点的直接信任值,则查询推荐信任值表,在推荐信任值表中,找到一个节点来作为推荐节点,推荐节点必须是与信任客体有过直接信任关系的节点,信任主体再根据该推荐节点的推荐信任值来进行抉择。

(2) 域间信任关系基于域间节点的交易。

域间信任值是域间节点的直接信任值和其他域的推荐信任值的综合。每个网格域都设置信任代理,域代理负责维护域间信任关系表和本域内所有节点的权值表。其中,域间信任关系表存储与本网格域有过直接交易的网格域的整体信任值。计算方法是域  $i$  内与该域有过交易的节点对域  $j$  的信任评估值与该节点权值<sup>[5]</sup>乘积的加权和。域  $i$  某个节点对域  $j$  的某个节点的信任值是由域间信任关系表中存储的域  $j$  的整体信任值与从其他域的代理收到的推荐信任值的加权和。

● 基于行为的信任模型的优点:

(a) 对于域内信任关系和域间信任关系使用不同的策略来处理,考虑比较全面,也较符合实际情况。

(b) 算法复杂度较小。

● 此信任模型的缺点:

(a) 上下文环境是决定信任的一个必要因素,但是此模型并没有考虑交易上下文;

(b) 没有充分体现出网格节点的信任自主,而且不论双方之前是否有过交易行为,属于不同网格域的节点在每次交易行为都要严格按照域间信任选择的步骤进行,这样使得操作过于繁琐;

(c) 没有给出系统初值的建立方法,且未考虑时间衰减;

(d) 域内推荐节点的诚实度未设置,且对其他域

的推荐信任的推荐权也未设置,导致在选取信任哪个节点或者域的推荐值时不易选择;

(e)没有考虑节点可能是属于多个信任域的。

### 3.2 改进的网格环境下的信任模型

通过对网络安全问题和现有信任模型的研究与分析,文中提出以下改进的信任模型基本框架:

(a)仍然采用上述信任模型,将信任关系分为域内和域间信任关系。

(b)节点存储直接信任指标,表中存储与域内本节点有直接交易的节点的信任值,当节点与已交易过的节点再次进行交易时,可以直接查询本地信任关系表,然后进行信任抉择,直接决定与此节点交易或者不交易,不需要询问代理。代理负责域间的信任管理,可降低域内节点对代理的依赖程度,避免网络瓶颈。

(c)在建立本地管理策略和安全策略的同时,建立信任表,设置信任值为某一固定值,并设置信任值阈值为 $\varepsilon$ ,信任值应大于等于 $\varepsilon$ ,若信任值在交易行为中小于 $\varepsilon$ ,则不再信任该恶意节点,并采取一定的惩罚措施。

(d)设置合适的衰减函数,充分考虑时间因素对信任值的影响。

(e)设置诚实度,使得节点在抉择时有更多、更可靠的自主选择。

图 1 是改进后模型的基本框架。

节点的职能<sup>[6]</sup>:本地存储直接信任值表和推荐信任值表,并对其进行维护和更新,不用询问域代理而自行判断做出信任抉择,进行信任推荐及交易结束后向域代理上报交易对象的信任值。

域代理的职能<sup>[7,8]</sup>:对节点加入域的请求进行处理,根据节点的不同身份决定节点的信任初值;维护及更新域内节点信任值表和域间信任关系表;与其他域代理进行信任交流;回答本域内节点信任值的询问;域内节点信任值表存储域内所有节点最近一次交易行为所产生的信任值,域间信任关系表中存储与该域有过

直接交易的域的整体信任值。

文中信任抉择采取三级受理的方式<sup>[9]</sup>。

具体过程如下:

信任主体节点在接到交易申请后,首先查找本地存储的直接信任值表,若存在对应记录则直接进行信任抉择;若不存在对应的记录,或者虽然存在对应的交易记录但是交易类型非本次交易类型的,则需要先判断交易双方节点是否属于同一个网格域的,若是同域的节点则将查找交易类型转换为信任推荐,在本地存储的推荐信任值表中查找与信任客体节点有过直接信任关系的直接信任值及其诚实度,利用推荐信任值公式计算信任客体的推荐信任值。如果无法找到这样的节点,则询问域代理,域代理收到请求后,在域内节点信任关系表中查找信任客体节点的信任值,然后进行回复;若非同域节点则询问域代理,域代理向其他域发出信任请求,由信任客体节点归属域的域代理回复询问节点(即信任主体节点)所属域的域代理,信任主体所属域的域代理得到回复后回复信任主体节点。若交易双方是之前有过信任关系的不同网格域的节点,则由交易服务方询问本域代理,查询对方域的整体信任值,再结合本地直接信任表中存储的信任客体节点的最近一次交易的直接信任值,计算出本次交易的直接信任值,此信任值为域间直接信任值;若交易双方是从未有过信任关系的不同域的节点,则由交易服务方代理询问对方代理,由对方代理提供交易申请节点的推荐信任值,再结合本域内与交易申请节点有过信任关系的节点的所有直接信任值,计算得出域间推荐信任值。这样按照“先本地、再同域、最后其他域”的步骤逐级地处理交易请求,使得交易处理操作有条不紊的进行。

### 3.3 信任关系计算

文中根据用户在网格中的交易行为成功或失败来计算用户的信任度,并根据用户的信任度这一属性来动态地授予访问资源的权限。

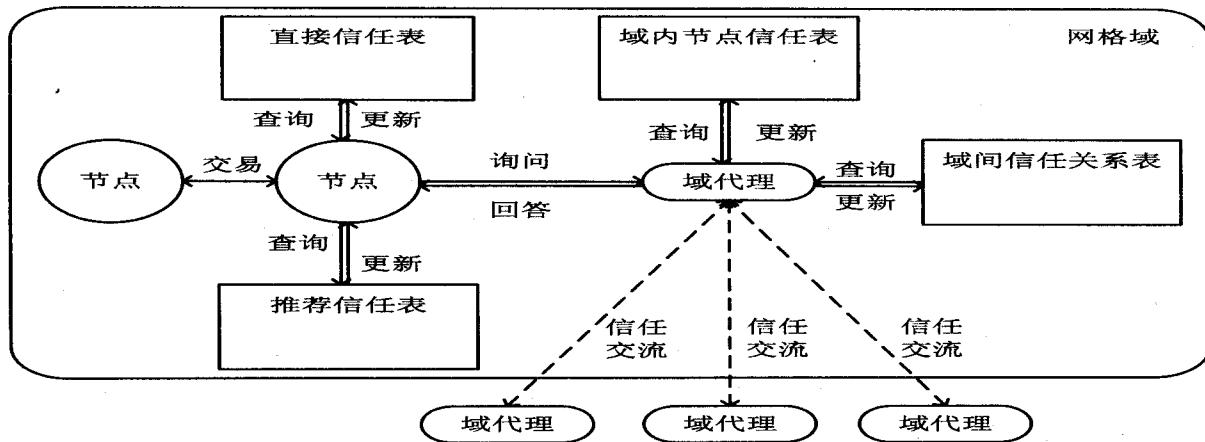


图 1 信任模型基本框架

信任值(Trust Value): 是信任关系的一种定量表示, 信任值可以用直接信任值和推荐信任值来综合衡量<sup>[10]</sup>, 用符号“T”来表示。

直接信任值(Direct Trust Value): 表示对实体间的直接即不通过第三方的信任的评估结果, 用符号“Dt”来表示。

推荐信任值(Recommendation Trust Value): 表示第三方向信任主体提供对信任客体的评估结果, 用符号“Rt”来表示。

在建立表时将直接信任值的初始值设定为某一固定值, 该初始值应大于信任值阈值  $\varepsilon$ , 若在交易行为中信任值小于  $\varepsilon$ , 则将此节点视为恶意节点, 禁止与其他的交易行为。

(1) 域内节点信任值的计算。

域内节点直接信任值的计算:

$$DT_{xy}(c, t) = DT_{xy}(c, t_0) \times C_{xy}(c, t - t_0) \quad (1)$$

其中,  $DT_{xy}(c, t)$  表示节点  $x$  和节点  $y$  在某一时刻  $t$  关于交易  $c$  的直接信任值,  $C_{xy}(c, t - t_0)$  为时间衰减因子。

域内推荐信任值的计算:

$$RT_y(c, t) = \frac{(1 - \lambda) \sum_{k=1}^n RT_{yk}(c, t_0) * C_{yk}(c, t - t_0) + \lambda TR_k}{n} \quad (2)$$

其中,  $RT_y(c, t)$  为在某一时刻  $t$ , 节点  $x$  和节点  $y$  要进行一项交易  $c$  时, 节点  $x$  计算节点  $y$  的推荐信任值,  $RT_{yk}(c, t_0)$  为节点  $k$  关于某项交易  $c$  向节点  $x$  提供节点  $y$  的推荐信任值,  $C_{yk}(c, t - t_0)$  为时间衰减函数,  $TR_k$  为节点  $k$  的诚实度,  $\lambda (0 \leq \lambda \leq 1)$  为加权因子, 用来调整推荐信任值对  $TR_k$  的偏重程度<sup>[11]</sup>。

域内信任值的计算:

在某一时刻  $t$ , 节点  $x$  和节点  $y$  要进行一项交易  $c$  时, 节点  $x$  要对节点  $y$  的信任值进行评估, 记该信任值为  $T_{xy}(c, t)$ 。信任值由直接信任值和推荐信任值组成, 故有:

$$T_{xy}(c, t) = \alpha \times DT_{xy}(c, t) + (1 - \alpha) \times RT_y(c, t) \quad (3)$$

其中,  $\alpha (0 \leq \alpha \leq 1)$  为加权因子, 通过加权因子  $\alpha$ , 可以根据实际情况调整  $T_{xy}(c, t)$  的获得更侧重于  $DN_y(c, t)$  还是  $RT_y(c, t)$ 。

(2) 域间信任值的计算。

不同网格域  $i$  和  $j$  中的节点  $X$  和  $Y$  进行交易时, 节点  $X$  归属于域  $i$ , 节点  $Y$  归属于域  $j$ , 节点  $X$  与节点  $Y$  的域间直接信任值计算方法如下:

$$D_{xy}(c, t) = (1 - \lambda) D_j(c, t_0) + \lambda D_{xy}(c, t_0) \times$$

$$C_{xy}(c, t - t_0) \quad (4)$$

$$\text{其中, } D_j(c, t_0) = \frac{\sum_{k=1}^n D_k(c, t_0) \times C_k(c, t - t_0)}{n} \text{ 表示}$$

域  $j$  的整体信任值, 是域  $j$  代理所管理的域内节点信任表中所有节点最近一次交易行为所产生的信任值的总和;  $D_{xy}(c, t_0)$  是节点  $X$  和节点  $Y$  在  $t_0$  时刻交易时的直接信任值。

域  $i$  中节点  $X$  与域  $j$  中节点  $Y$  无直接信任关系时用以下公式计算域间推荐信任值:

$$R_{xy}(c, t) = (1 - \lambda) \frac{\sum_{k=1}^n DT_{yk}(c, t_0) \times C_{yk}(c, t - t_0) + TR_k}{n} + \lambda RT_{yl}(c, t_0) \quad (5)$$

其中,  $D_{yk}(c, t_0)$  表示域  $i$  中与节点  $Y$  交易过的节点的直接信任值,  $C_{yk}(c, t - t_0)$  为时间衰减函数,  $TR_k$  为节点  $k$  的诚实度,  $RT_{yl}(c, t_0)$  表示域  $j$  内节点  $Y$  的推荐信任值, 由公式(2) 计算得出;  $\lambda (0 \leq \lambda \leq 1)$  为加权因子。

(3) 时间衰减函数。

上述公式中引入了时间衰减因子, 信任值会随着时间而衰减, 其衰减速率会受多方面的影响, 参考文献[12] 中的表示形式, 它具有一定的通用性。

$$C_{yk}(c, t - t_0) = \frac{1}{1 + ((t - t_0) / S(c, D_x, D_y, \dots))} \quad (6)$$

其中,  $S(c, D_x, D_y, \dots)$  为衰减速率, 与多种因素有关, 实际运用时视具体情况而定。

### 3.4 实验验证及分析

文中提出的网格信任模型中, 网格域代理要先建立自己的管理策略和安全策略, 包括本域的各节点的信任值表, 然后建立与其他域的域间信任关系表。按照模型架构将信任关系划分层次, 根据不同的信任关系, 利用审计数据和入侵检测系统对被评估域的行为进行评估, 完成信任值的计算, 更新信任值表。

为了验证文中信任模型的有效性, 进行以下模拟仿真实验: 设计 100 个网格域, 每个网格域包含 10 个实体, 分别在普通信任模型和改进后的信任模型中进行 10000 次交互, 既有同域实体间的交互, 也有不同域实体间的交互, 可能进行恶意推荐的占 20%, 实验后对两种情况进行对比分析, 见图 2。

通过普通信任模型和改进后的信任模型的对比实验可以看出, 改进后的信任模型虽然在试验初期的交易成功率较低, 但是随着交易次数的增多、环境的稳定以及其他因素的影响, 交易成功率逐渐提高, 比普通模

型的交易成功率有了较大的提升,说明本信任模型能够较有效地提高交易成功率,有效地抑制恶意节点的行为,改善网络性能。实验结果证明了该信任模型的可行性和有效性。

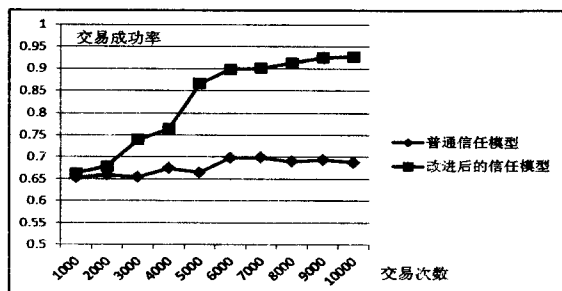


图 2 普通模型和改进后的信任模型交易成功率

#### 4 结束语

文中针对网络安全的特点,研究了网络安全中的信任关系和已有的网格信任模型,并对其进行改进,将信任值分类细化,并分别给出了域内直接信任值、推荐信任值及域间直接信任值、推荐信任值的计算方法,在计算值时引入时间衰减因子和加权因子,使得节点在抉择时更为客观。通过模拟实验证明了该模型的可行性,下一步的工作是给出合理的时间衰减函数以及加权因子的选取方法,同时完善自动更新机制,考虑节点可能属于多个信任域的情况,进一步提高交易的成功率,降低交易失败的风险,使得此网格信任模型更加实现网络的动态性和安全性。

(上接第 35 页)

少,甚至还会降低。尽管语速对元音和辅音的运动速度产生了不同的影响,但最大速度与运动距离比值的增量却是大致相同的。

#### 参考文献:

- [1] Zhang Shaobai, Ruan Xiaogang, Cheng Xiefeng. A new constructing method of cerebellum model applying to DIVA model [C]//Control and Decision Conference, CCDC 2009. Guilin, Chinese; [s. n.], 2009.
- [2] Lacer F, Klintfors E, Gustavsson L. Multisensory information as an improvement for communication systems' efficiency [C]//Proceedings from Fonetik 2005. Gothenburg, Sweden; [s. n.], 2005.
- [3] Guenther F H, Ghosh S S. A model of cortical and cerebellar function in speech [C]//Proceedings of the XVth International Congress of Phonetic Sciences. Barcelona; [s. n.], 2003: 169-173.
- [4] Guenther F H, Perkell J S. A neural model of speech production and its application to studies of the role of auditory feed-

#### 参考文献:

- [1] 朱春鸽. 网络环境下信任的研究与应用 [D]. 北京: 北京邮电大学, 2007.
- [2] Beth T, Borchering M, Klein B. Valuation of trust in open networks [C]//Proceedings of the European Symposium on Research in Security (ESORICS). Brighton; Springer-verlag, 1999: 59-63.
- [3] 黄刚, 王汝传, 田凯. 基于 RBAC 策略的可信网络访问控制模型 [J]. 计算机应用研究, 2010, 27(4): 1473-1476.
- [4] 王莉苹, 杨寿保. 网络环境中的一种信任模型 [J]. 计算机工程与应用, 2004, 40(23): 50-53.
- [5] 王东安. 网络计算中信任模型及其应用研究 [D]. 北京: 中国科学院研究生院, 2006.
- [6] 杨璐. 基于信任域的网格信任模型研究 [D]. 西安: 西北大学, 2008.
- [7] 邓勇, 张琳, 王汝传, 等. 网络计算中基于信任度的动态角色访问控制的研究 [J]. 计算机科学, 2010, 37(1): 51-54.
- [8] 张亮. 网络安全中信任关系以及访问控制的研究 [D]. 合肥: 合肥工业大学, 2007.
- [9] 李文娟, 王晓东, 傅仰耿, 等. 几种网络信任模型的研究 [J]. 福州大学学报 (自然科学版), 2006, 34(1): 189-193.
- [10] 王晓华. 网络环境下基于行为的信任模型研究 [D]. 济南: 山东大学, 2009.
- [11] 姚寒冰. 网络环境中访问控制与信任模型研究 [D]. 武汉: 华中科技大学, 2006.
- [12] 高承实, 王建政, 沈昌祥, 等. 网络环境下层次信任模型研究 [J]. 计算机工程与应用, 2007, 43(13): 132-136.

back in speech [M]//Speech Motor Control in Normal and Disordered Speech. Oxford: Oxford University Press, 2004: 29-49.

- [5] 杜华英, 赵跃龙. 人工神经网络典型模型比较研究 [J]. 计算机技术与发展, 2006, 16(5): 1-3.
- [6] Guenther F H, Hampson M, Johnson D. A theoretical investigation of reference frames for the planning of speech movements [J]. Psychol Rev, 1998, 105: 611-633.
- [7] 刘雅琴, 智爱娟. 几种语音识别特征参数的研究 [J]. 计算机技术与发展, 2009, 19(12): 67-70.
- [8] 王晓敏, 刘希玉, 戴芬. BP 神经网络预测算法的改进及应用 [J]. 计算机技术与发展, 2009, 19(11): 64-67.
- [9] 林联明, 王浩, 王一雄. 基于神经网络的 Sarsa 强化学习算法 [J]. 计算机技术与发展, 2006, 16(1): 30-32.
- [10] 葛哲学, 孙志强. 神经网络理论与 MATLAB R2007 实现 [M]. 北京: 电子工业出版社, 2007.
- [11] 钟淑瑛, 李陶深. 基于 MATLAB 的 BP-LVQ 神经网络组合分类模型 [J]. 计算机技术与发展, 2006, 16(2): 114-116.
- [12] Guenther F H. Neural models of adaptive sensory-motor control for flexible reaching and speaking [D]. Boston, MA: Boston University, 1992.