计算机科学 2007Vol. 34№. 1

视觉跟踪模糊自调节 PI 控制算法

沈晓晶　陈　明　李　净　池　涛
（上海水产大学信息学院　上海 200090）

摘　要　视觉跟踪系统是一个非线性时变系统，传统控制方法往往难以胜任。因此，本文提出一种新的视觉跟踪控制算法——模糊自调节 PI 控制算法，以跟踪三维平动刚体目标。与传统基于图像的视觉伺服控制算法相比，该控制算法有两个优点：①以二值目标图像的矩特征为图像特征，因而无需图像特征匹配；②模糊调节器根据闭环系统响应的不同阶段，在线调节 PI 参数，从而改善了闭环系统的整体性能。仿真结果表明，本文提出的模糊自调节 PI 控制算法不仅简单快速，且具有较高控制精度。

关键词　视觉跟踪，图像雅可比，PI 控制，模糊调节

Fuzzy Self-Tuning PI Control Algorithm for Visual Tracking

SHEN Xiao-Jing　CHEN Ming　LI Jing　CHI Tao
(College of Computer Science, Shanghai Fisheries University, Shanghai 200090)

Abstract　Visual tracking systems are often nonlinear and temporal systems, which are hard to be treated by the traditional control methods. This paper proposes a fuzzy self-tuning PI control algorithm for a visual tracking system to track a rigid planar object in 3D translational motion. Compared with traditional image-based visual servoing methods, this algorithm has two advantages: ①Image feature match is unnecessary as binary image moments are selected as image features, and thus image processing is simplified; ②According to the fuzzy rules, PI parameters varies in the different stage of the closed system response. Simulation results show that the control algorithm proposed in the paper is not only simple and fast, but performs well.

Keywords　Visual tracking, Image jacobian matrix, PI control, Fuzzy tuning

1　前言

视觉跟踪问题涉及广泛[1,2]，对它的研究常见于自动导航、自动监控及机器人等领域中。

本文主要研究一平面刚体目标在三维笛卡儿空间做三维平动时，摄像机从任意位置开始对该运动目标进行视觉跟踪的问题。本文基于目标为平面刚体且做三维平动的假设，寻找一种相对简单的 IBVS(基于图像的视觉伺服)控制算法。与传统 IBVS 方法不同，我们采用二维图像中的目标质心投影以及三维空间中的目标深度比来反映在目标在其运动空间的三维位置。此外，考虑到视觉跟踪系统是一个非线性系统，其控制过程具有高度的非线性和时变性。因此，我们引入模糊控制器对视觉跟踪控制器的 PI 参数进行在线调节，优化系统整体性能。

本文首先介绍一种图像平动仿射模型，接着从该模型出发，推导出图像雅可比矩阵，然后基于图像雅可比矩阵设计用于视觉跟踪的模糊自调节 PI 控制器，最后给出该算法的仿真结果。

2　图像运动仿射模型

如图 1 所示建立两参考坐标系：摄像机坐标系{C}，其原点 O 设在透镜中心；图像坐标系{I}，其原点 o 设于图像中心。

设：坐标系{C}中，P 为目标上任一点，其坐标为$[X,Y,Z]^T$；P 投影在图像上的点为 p，其在坐标系{I}中的坐标为$[x, y]^T$。摄像机模型采用针孔模型，投影变换公式为[1]：

$$x=(fXk_x)/Z, y=(fYk_y)/Z \tag{1}$$

式(1)中：f 为摄像机焦距，k_x、k_y 分别表示摄像机的水平、垂直比例因子。

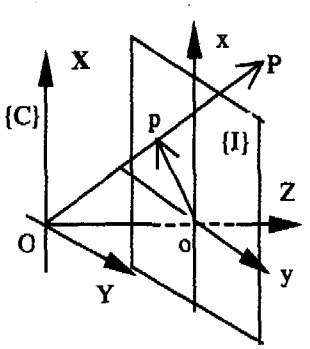


图 1　摄像机坐标系{C}和图像坐标系{I}

当目标静止而摄像机仅做平移运动时，则点 P 在坐标系{C}的位移可用以下模型描述[1]：

$$[X',Y',Z']^T=[X,Y,Z]^T-T \tag{2}$$

式(2)中：T 为平移矩阵，$T=[T_X,T_Y,T_Z]^T$；t 和 t'时刻，坐标系{C}中点 P 位置为$[X, Y, Z]^T$ 和$[X', Y', Z']^T$。

综合(1)和(2)式，点 p 在坐标系{I}中的位移可由以下仿射变换模型描述：

$$sx'=x-T_u, sy'=y-T_v \tag{3}$$

沈晓晶　讲师，主要研究方向：计算机视觉、图像处理、智能控制。

其中：$s=(Z'/Z)=1-(T_Z/Z)$，$T_u=(fk_xT_X)/Z$，$T_v=(fk_yT_Y)/Z$，$[x,\ y]^T$和$[x',\ y']^T$为t和t'时刻点p的坐标。

3 s的测量

定义1 设A为目标在图像坐标系$\{I\}$上的闭合投影区域，二值图像$f(x,y)$函数定义为：

$$f(x,y)=\begin{cases}1;(x,y)\in A\\0;(x,y)\notin A\end{cases}$$

则二维$(p+q)$阶图像矩的定义如下：

$$M_{pq}=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}x^py^qf(x,y)\mathrm{d}x\mathrm{d}y=\iint_{(x,y)\in A}x^py^q\mathrm{d}x\mathrm{d}y \quad (4)$$

若目标图像为数字图像，且其尺寸为$(N\times M)$个像素点，则二维$(p+q)$阶图像矩的计算公式为：

$$M_{pq}=\sum_{j=0}^{M-1}\sum_{i=0}^{N-1}j^pi^qf(i,j)\quad i=0,1,\cdots,(N-1),\ j=0,1,\cdots,(M-1) \quad (5)$$

引理1[4] 设M'_{00}和M_{00}分别为平面刚体在不同深度Z'和Z上得到的零阶图像矩。若平面与摄像机光轴垂直，则下列关系式成立：

$$s=Z'/Z=(M_{00}/M'_{00})^{1/2} \quad (6)$$

s实际上表示摄像机缩放效果，当目标为一始终垂直于摄像机光轴的平面刚体时，s可由二值目标图像的零阶图像矩获得。

4 视觉跟踪控制结构

由(6)式推导出(7)式：

$$Z_c=Z_ds=Z_d[(M_{00})_d/(M'_{00})_d]^{1/2} \quad (7)$$

式(7)中：Z_d、Z_c表示理想目标深度和当前目标深度；$(M_00)_d$表示理想目标图像的零阶矩(即目标在理想深度下获得的二值目标图像的零阶矩)；$(M_{00})_c$表示当前目标图像的零阶矩(即目标在当前深度下获得的二值目标图像的零阶矩)。

式(7)表明：若Z_d恒定，则通过测量s可间接获知目标深度变化。

已知目标为平面刚体，目标质心在图像平面上的投影位置可由式(8)估算出[3]：

$$x_c=M_{10}/M_{00},y_c=M_{01}/M_{00} \quad (8)$$

本文研究垂直于摄像机光轴的平面刚体在其运动空间作三维平动时的视觉跟踪控制问题。因此，我们选择向量$[x_c,\ y_c,\ s]^T$作为视觉跟踪控制系统的图像特征向量和状态向量，系统控制结构如图2所示。图2中：X^*表示系统状态向量的期望值，且$X^*=[x_c^*,\ y_c^*,s^*]^T=[0,\ 0,1]$。

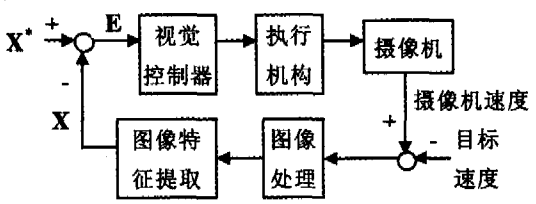


图2 视觉跟踪控制结构示意图

系统误差：

$E=[e_1,\ e_2,\ e_3,]^T=X^*-X=[-x_c,-y_c,(1-s)]^T$。当$|E|<\varepsilon$时，表示系统满足控制要求。

(7)和(8)式表明：$\{x_c,\ y_c,\ s\}$可通过二值目标图像的零、一阶矩特征估算出。因此，$\{x_c,\ y_c,\ s\}$实际上是图像矩特征集的一个子集。

5 受限"P+模糊自调节PI"控制律

对式(3)求导，得：

$$\dot{X}=J_vU \quad (9)$$

其中：$\dot{X}=[\dot{x}_c,\dot{y}_c,\dot{s}]^T$，$U=[T_X,T_Y,T_Z]^T/Z_d$。

$$J_v=\begin{bmatrix}s&0&x_c\\0&s&y_c\\0&0&1\end{bmatrix}^{-1}\cdot\mathrm{diag}(-fk_x,-fk_y,-1) \quad (10)$$

式(10)为图像雅可比矩阵J_v(反映三维摄像机运动与二维图像特征运动之间映射关系的矩阵)。

设：v_c为摄像机线速度，v_0为目标线速度，则有：$[T_X,\ T_Y,T_Z]^T=v_c-v_0$。若目标静止，由式(9)推知：

$$\dot{X}=(J_vv_c)/Z_d \quad (11)$$

为保证系统稳定性，利用Lyapunov函数设计视觉跟踪控制器。所选Lyapunov函数[3]为：

$$L=(E^TPE)/2 \quad (12)$$

对L求导，得：

$$\dot{L}=E^TP\dot{E} \quad (13)$$

对系统误差求导，有：$\dot{E}=-\dot{X}=-(J_vv_c)/Z_d$。

将上式代入式(13)，得：

$$\dot{L}=-E^TP(J_vv_c)/Z_d \quad (14)$$

$\dot{L}<0$，系统渐近稳定。因此，静止目标的视觉伺服控制律如式(15)所示：

$$v_c=\mathrm{diag}(fk_x,fk_y,1)J_v^{-1}KE \quad (15)$$

式(15)中：$K=\mathrm{diag}(k_1,k_2,k_3)$，$k_i>0(i=1,2,3)$

仿真结果表明：当目标作三维平运时，(15)式只能使系统静差趋于不为零的某个常数。

考虑在控制后期加入积分环节以消除系统静差，并增加限幅环节以限制摄像机线速度。为使系统获得满意的动态特性，采用模糊调节器实时调节PI参数。综上所述，视觉跟踪控制器采用受限"P+模糊自调节PI"控制算法。

对于离散系统，设系统采样时间为T_s，摄像机线速度各分量限值为100mm/s，k时刻，摄像机线速度为$[(v_X)_k,\ (v_Y)_k,\ (v_Z)_k]^T$，闭环系统误差为：

$$E_k=[(e_1)_k,\ (e_2)_k,\ (e_3)_k,]^T=[(-x_c)_k,\ (-y_c)_k,\ (1-s_k)]^T$$

根据(10)和(15)式，令：

$$(w_1)_k=s_k(e_1)_k+(x_c)_k(e_3)_k,$$

$$(w_2)_k=s_k(e_2)_k+(y_c)_k(e_3)_k,\ (w_3)_k=(e_3)_k$$

则受限"P+模糊自调节PI"控制算法描述如下：

(a)若$[|w_1|,|w_2|,|w_3|]^T>[TH_1,TH_2,TH_3]^T$，视觉跟踪控制器用受限P控制律，摄像机线速度为

$$(v_i)_k=\begin{cases}(v'_i)_k,\mathrm{if}|(v_i)_k|<100\\\mathrm{sgn}[(v'_i)_k]\cdot100,\mathrm{if}|(v_i)_k|\geqslant100\end{cases},$$

i表示X,Y,Z

$$(v'X)_k=-k_{PX}(w_1)_k,\ (v'_Y)_k=-k_{PY}(w_2)_k,$$

$$(v'_Z)_k=-k_{PZ}(w_3)_k$$

k_{PX}，k_{PY}，k_{PZ}均大于零 (16)

(b)若$[|w_1|,|w_2|,|w_3|]^T\leqslant[TH_1,TH_2,TH_3]^T$，视觉跟踪控制器用受限模糊自调节PI控制律，摄像机线速度为：

$$(R_h)_k=(R_h)_{k-1}+(w_h)_k,\ (R_h)_0=0,\ h=1,2,3$$

$$\begin{cases}(v'_X)_k=-(k_{PX})_k[(w_1)_k+T_s(R_1)_k/(T_{iX})_k]\\(v'_Y)_k=-(k_{PY})_k[(w_2)_k+T_s(R_2)_k/(T_{iY})_k]\\(v'_Z)_k=-(k_{PZ})_k[(w_3)_k+T_s(R_3)_k/(T_{iZ})_k]\end{cases}$$

$$(v_j)_k=\begin{cases}(v'_j)_k, \text{if}|(v_j)_k|<100\\ \text{sgn}[(v'_j)_k]\cdot 100,(R_l)_k=(R_l)_{k-1}, \text{if}|(v_j)_k|\geqslant 100\end{cases}$$

j 表示 $X,Y,Z,h=1,2,3,k=0,1,2,\cdots$

(17)

式(18)中：$k_{PX}(k)$与 $T_{iX}(k)$，$k_{PY}(k)$与 $T_{iY}(k)$，$k_{PZ}(k)$与 $T_{iZ}(k)$，分别由 3 个独立的模糊调节器在线调节。

6 模糊调节器

取系统误差 E 和误差变化 EC 为模糊控制器的输入语言变量，增益变化 k_pC 和积分时间变化 T_iC 为输出语言变量。每个变量取三个语言值“负(N)”、“零(Z)”、“正(P)”。语言变量 E、EC、k_pC 和 T_iC 的隶属函数均为三角函数。

令 E、EC、k_pC 和 T_iC 的论域均为$[-1,1]$，并用量化因子(k_E，k_{EC})和比例因子(k_{uP}，k_{ui})分别对模糊调节器的输入量和输出量进行数值变换。PI 参数调节公式为：

$$\begin{aligned}k_P(k)&=k_P(k-1)+k_{uP}\Delta k_p(k)\\ T_i(k)&=T_i(k-1)+k_{ui}\Delta T_i(k)\end{aligned}\tag{18}$$

注意：$\Delta k_P(k)$和 $\Delta T_i(k)$为 k 时刻模糊调节器的精确输出量，与之对应的语言变量分别是 k_pC 和 T_iC。

如果 $k_P(k)$，$T_i(k)$的取值范围如下：

$k_p\in[k_{p\_\min}, k_{p\_\max}]$，$T_i\in[T_{i\_\min}, T_{i\_\max}]$

则 PI 参数初值可取：

$$k_p(0)=(k_{p\_\max}+k_{p\_\min})/2, T_i(0)=(T_{i\_\max}+T_{i\_\min})/2\tag{19}$$

下面讨论模糊规则的设计。本文基于闭环系统响应曲线设计 PI 参数模糊调节规则。

如图 3 所示，闭环系统误差曲线可分为 A～E 五个曲线段，分别对应闭环响应过程中的 5 个阶段。图中，$e(k)$表示闭环系统误差，$\Delta e(k)$表示闭环系统误差的变化量：

曲线 A，$e(k)>0$ 且 $\Delta e(k)<0$；曲线 B，$e(k)<0$ 且 $\Delta e(k)<0$；

曲线 C，$e(k)<0$ 且 $\Delta e(k)>0$；曲线 D，$e(k)>0$ 且 $\Delta e(k)>0$；

曲线 E，$e(k)\approx 0$ 且 $\Delta e(k)\approx 0$；

过零点 b，$e(k)=0$ 且 $\Delta e(k)<0$；

过零点 d，$e(k)=0$ 且 $\Delta e(k)>0$。

通常希望闭环系统的超调量(σ_p)，调节时间(t_s)，和上升时间(t_r)越小越好。

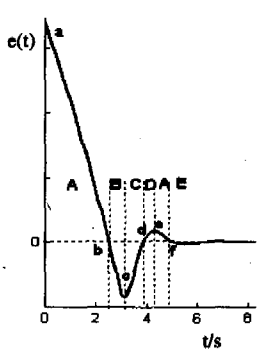


图 3 闭环系统误差曲线

因此 PI 参数调节规则的语言描述如下[5]：

曲线段 A：增加 $k_p(k)$且减小 $T_i(k)$，以增大输出、减小 t_r；点 b：减小 $k_p(k)$且增大 $T_i(k)$，为减小输出和 σ_p 做准备；曲线段 B 和 C：减小 $k_p(k)$且增大 $T_i(k)$，以进一步减小 σ_p；点 d：增加 $k_p(k)$且减小 $T_i(k)$，为增大输出和减小 t_s 准备；曲线段 D：增加 $k_p(k)$且减小 $T_i(k)$，以增大输出和减小 t_s；曲线 E：保持 $k_p(k)$和 $T_i(k)$不变。

根据上述调节规则，设计 k_pC 和 T_iC 的模糊调节规则表(见表 1、表 2)。模糊规则表述形式为：

if E is E_i and EC is dE_j, then k_pC is C_{ij} and T_iC is D_{ij}。

表 1 k_pC 模糊调节规则

E \ EC	N	Z	P
N	N	P	N
Z	N	Z	P
P	P	N	P

表 2 T_iC 模糊调节规则

E \ EC	N	Z	P
N	P	N	P
Z	P	Z	N
P	N	P	P

例如，表 1 中的第一行第一列与表 2 中的第一行第一列对应，形成一条模糊规则如下：

if E is N and EC is N, then k_pC is N and T_iC is P

模糊逻辑推理采用 mamdani 方法(即“min-max”型推理方法)，解模糊判决采用重心法。

7 仿真结果

设：系统采样时间 $T_s=100$ms；摄像机参数：$f=16$mm，$k_x=40.25$pixels/mm，$k_y=37.21$pixels/mm。

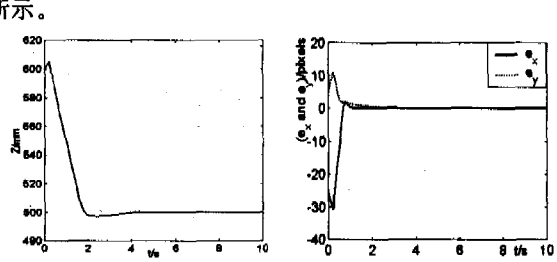
其他仿真条件：(a)理想目标深度，$Z_d=500$mm，与 Z_d 相对应的理想二值目标图像的零阶矩，$(M_{00})d=10506$；(b)初始状态下摄像机摄取一幅目标图像，其二值图像的零阶和一阶矩特征为：

$[M_{10}, M_{01}, M_{00}]^T=[182750, -36550, 7310]^T$。

由(7)和(8)式估算出系统的初始状态向量值为：

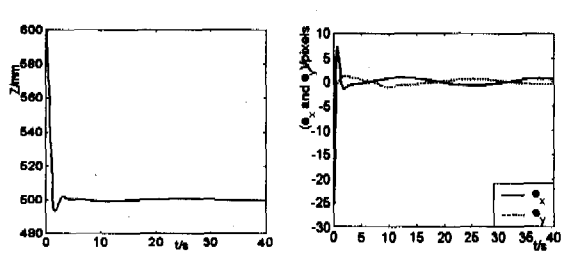
$X_0=[(x_c)_0, (y_c)_0, s_0]^T=[25,-5,1.1988]^T$。

采用受限“P+模糊自调节 PI”控制律((16)～(19)式，表 1、2 中的模糊调节规则)，系统跟踪匀速平动目标的仿真结果如图 4 所示。



(a) 目标深度变化曲线　(b) 目标质心位置误差

图 4 匀速直线运动目标的视觉跟踪仿真结果



(a) 目标深度变化曲线　(b) 目标质心位置误差

图 5 缓慢变速平动目标的视觉跟踪仿真结果

当目标在其运动空间作缓慢的变速平动，且 $v_{OX}=v_{OZ}=30\sin(0.04t)$，$v_{OY}=-30\sin(0.04t)$。在受限“P+模糊自调节

PI"控制律作用下，系统对运动目标进行视觉跟踪的仿真结果如图5所示。

分析图4与图5知：当目标匀速运动或作缓慢变速平动时，在受限"P+模糊自调节PI"控制律的作用下，目标深度和目标质心在图像上的投影位置可快速收敛至理想值附近，即目标深度收敛至理想深度500mm附近，目标质心投影位置收敛至图像中心$[0,0]^T$附近。并且由于模糊调节器的在线调节功能，控制系统具有较好的动态特征。

结束语 本文阐述了一种能跟踪匀速平动或者缓慢变速平动目标的视觉伺服控制结构和PI参数模糊自调节的视觉跟踪控制算法。在该控制结构和控制算法的作用下，目标始终保持在图像中央且目标深度满足给定值。此外，本文所选择的图像特征集实际上为二值目标图像矩特征的一个子集。采用图像矩作为图像特征的好处是：①无需特征匹配，简化图像处理过程；②对图像噪声具有较强的鲁棒性。

参考文献

1 Hutchinson S. A Tutorial on Visual Servo Control. IEEE Transactions on Robotics and Automation, 1996,12:651～670

2 Benameur K, Belanger P R. Grasping of a moving target with a robotic hand-eye system. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, 1998. 304～310

3 林靖，陈辉堂，王月娟，等. 基于图像矩的运动目标3D平动视觉跟踪. 机器人，2000,22:218～223

4 SHEN Xiao-Jing. A Simple Adaptive Control for Visual Servoing, 2003 International Conference on Machine Learning and Cybernetics, November 2003,2: 976～979

5 Hong Hyeong-Pyo, Park Suk-Joon, Cho Kyeong-Young. A design of auto-tuning PID controller using fuzzy logic. In: Proceeding of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation, Nov. 1994, 2: 971～976

(上接第116页)

中$(n-t)$的个服务器被攻占或失效，任意用户$U_j \in U$都可向剩余的t个服务器提出请求，同样可以获得t个秘密分片从而恢复会议密钥K。同时，被攻占的$(n-t)$个服务器因为少于t个，所以无法重构多项式$y \equiv f(x) \pmod q$，从而无法获得K的任何信息。

4.2 抗欺诈性分析

本方案可抵抗网络内外的各种欺诈行为：(1)假冒发起者的欺诈：任何非法用户(即没有建立公私钥对的用户)想假冒合法用户发起会议。由于没有正确的私钥D_d，将不能通过验证：$\hat{e}(h_2(R)D_i, Q_d) \stackrel{?}{=} \hat{e}(h_2(R)Q_i, D_d)$，因此任何$U_i \in S$将发现这种欺骗。(2)假冒服务器的欺诈：任何$U_s \notin S$想假冒服务器成员，他可在密钥分发中计算$h_2(R)D_i$，或者在密钥重构中计算$\hat{e}(h_2(R)D_d, D_i)$时欺骗，但是由于$h_2(R)$和$h_2(R)D_d$都是公开信息，任何成员都可以利用$U_i$的公钥$Q_i$进行验证，发现其欺诈行为。(3)假冒会议成员的欺诈：由于每一个服务器成员都秘密地拥有被邀请成员的信息U，任何$U_i \notin U$想假冒会议成员来非法获得会议密钥，都不能通过服务器的检验。(4)不诚实服务器的攻击：如果服务器提供不正确的私钥来生成签名或解密，和(2)一样，将不能通过验证。

另外，由于每个服务器都保存有会议密钥的有效期(T_0+T_d)，当会议过期时，每个服务器都会拒绝为任何成员提供重构会议密钥的服务，这样，就实现了会议密钥的撤消。

4.3 网络性能分析

本方案具有可扩展性的优点，与Tzeng和Xu的方案相比，更适合应用于分布式的环境中。主要表现在这几个方面：(1)会议密钥的秘密分片由服务器自身的私钥产生，在密钥的分发过程中，每个服务器的私钥不会被任何其它成员计算出来，当有多个会议密钥需要共享时，每个会议密钥在这个服务器上的秘密分片只由会议发起者产生的随机数和其本身的私钥决定，不能互相计算得到。这样，任意合法成员都可发起会话，也可在各自指定的服务器集中共享多个会议密钥，同时不需要专门的服务器来存储其秘密分片。(2)服务集S可由会议发起者指定，一般根据选择那些能稳定地提供网络服务的成员作为服务器。服务集的规模n根据它们与会议发起者之间的链路状态来选定，而t值则由会议发起者通过综合考虑网络的运行效率和会议的安全性给出。

结论 本文利用基于身份的密码体制和Shamir秘密共享方案，提出了一种分布式会议密钥分发方案。与传统的秘密共享方案不同的是，秘密分片由服务器的私钥产生，通过收集这些秘密分片，构造多项式函数。这样不需要由会议发起者分发秘密分片，并且在会议密钥的分发和重构过程中，各个成员的身份可以方便地进行验证，避免了各类欺诈行为的发生。与传统的集中式会议密钥分配方案相比，避免了其单一失败点的问题，同时，比协商式会议密钥分配方案具有更少的通信开销和更好的可扩展性，更适合应用于分布式网络。

参考文献

1 Hwang M S. Dynamic Participation in A Secure Conference Scheme For Mobile Communications. IEEE Trans. Vehicular Technology, 1999, 48(5): 1469～1474

2 Xu Y, Siew C K, Tan C H. A Secure and Efficient Conference Scheme for Mobile Communications. IEEE Trans. Vehicular Technology, 2003, 52(4): 784～793

3 Chang C C, Wu T C, Chen C P. The Design of a Conference Key Distribution System. In: Proc. Advances in Cryptology-Auscrypt'92, 1992. 459～466

4 Steiner M, Tsudik G, Waidrer M. Diffie-Hellman key distribution extended to groups. In: ACM Conference Computer and Communication Security, California, 1996, 3: 31～37

5 Kim Y, Perrig A, Tsudik G. Group Key Agreement Efficient in Communication. IEEE Trans. Computers, 2004, 53(7): 905～921

6 Tzeng W G. A Secure Fault-tolerant Conference-key Agreement Protocol. IEEE Trans. Computers, 2002, 51(4): 373～379

7 Xu Y. Identity-Based Fault-Tolerant Conference Key Agreement. IEEE Trans. Dependable and Secure Computing, 2004, 1(3): 170～178

8 Shamir A. Identity-based Cryptosystems and Signature Schemes. In: Proceedings of Crypto 1984, Providence, USA: Springer-Verlag, 1984. 47～53

9 Shamir A. How to Share a Secret. Comm. ACM, 1979, 22(11): 656～715

10 Verheul E R. Evidence That XTR Is More Secure Than Supersingular Elliptic Curve Cryptosystems. Advances in Cryptology-Proceedings of EUROCRYPT'01, Spring-Verlag, 2001. 195～210

11 Boneh D, Franklin M. Identity Based Encryption From The Weil Pairing. Advances in Cryptology-Proceedings of CRYPTO'01, Spring-Verlag, 2001. 213～229