

## 网络信任评价审计及控制

何延年,马满福,李 勇,曲伟丽

(西北师范大学 数学与信息科学学院,兰州 730070)

(hetn@nwnu.edu.cn)

**摘 要:**客观地评价资源是信任模型有效的基础,而评价的主观性则使其难以实现,审计成为维护评价客观性的重要方法。针对信任评价,提出了一个带有审计功能的评价模型,通过采集调度数据、标准化、距离计算、异常评价发现和评价修正等步骤,实现评价的审计和对评价的控制。讨论了审计周期,给出了审计算法。实验表明,所提出的方法对用户信任评价的审计是有效的,发现了评价中存在的问题并在后来的评价中加以修正,同时促进了系统的稳定性和吞吐量。

**关键词:**网络监测体系结构;信任模型;欧式距离;资源使用记录

**中图分类号:** TP302 **文献标志码:** A

## Audit and control of trust evaluation in grid

HE Ting-nian, MA Man-fu, LI Yong, QU Wei-li

(College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu 730070, China)

**Abstract:** Objective evaluation of trust value is the basis of trust model validity, but the subjectivity of evaluation makes it hard to achieve. Audit is one of the effective ways to this problem. In this paper, the authors presented an approach of trust evaluating model with audit function, by the support of basis running data. The process included standardization, distance calculating, and abnormality evaluation detecting and correcting, thus implementing the control of evaluation. As to the model requirement, the authors analyzed the refresh periods of audit, and an audit algorithm was put forward. Finally simulations were performed to validate the audit. The experimental results show that the audit is efficient on trust model stability and at the same time is helpful with the throughput of grid.

**Key words:** Grid Monitoring Architecture (GMA); trust model; Euclidean distance; Resource Usage Record (RUR)

## 0 引言

信任模型为提高资源的可靠性而进行信任评价,但存在以下两方面的问题:1)用户评价的主观性和随意性;2)模型自身缺乏可靠性。由于评价的主观性和随意性,使得用户评价缺乏约束,给一些合谋者进行信任度欺诈提供了方便,也使不良用户诋毁其他实体者大行其道。模型自身缺乏可靠性则使得恶意和不良评价直接影响到模型的正常运行,进而导致网络系统缺乏稳定性,严重影响系统效率。信任模型面临恶意欺诈、合谋、诋毁等不端行为的严重困扰<sup>[1]</sup>。在信任评价缺乏控制的同时,网络监测、网络监测以及运行日志等采集了大量的原始数据,蕴涵了对网络进行评价的各种要素。如何利用这些数据,对网络从管理、调度到信任等的审计是关系到进一步推进网络系统稳定性的基础性问题。当前审计在网络中的研究主要针对安全展开,用来在线进行入侵检测<sup>[2-3]</sup>;从网络管理角度的相关研究主要包括全球网络论坛提出的网络监测体系结构(Grid Monitoring Architecture, GMA)<sup>[4]</sup>,以及在其基础上提出的各种实现<sup>[5]</sup>;从信任可靠性和稳定性方面的研究有非正常评价过滤等方法<sup>[6]</sup>。对管理、调度以及信任评价等的审计还看不到相关文献。针对上述现状,本文尝试利用这些基础数据,实现对网络信任评价的审计,进而影响信任

策略,提高信任评价的准确性和模型的抗风险能力。

## 1 审计数据支撑

审计以网络监测、网络监控等数据为依据,一般来说,一个网络管理域和一个局域网在管理范围上是一致的,因此这些数据便于得到。另外,监测数据获取可以简单地跨越网络和网络层次的概念,从不同的层面得到。审计数据支撑如图1所示。

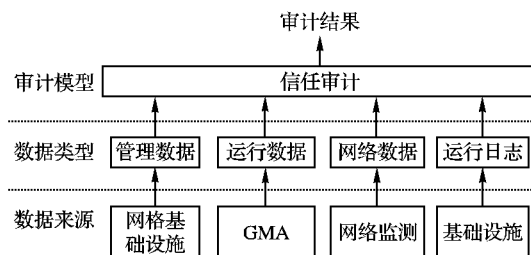


图1 信任审计数据支撑结构

数据类型包括以下4类:1)管理数据。它们存放在域内的基础设施上,包括资源和用户注册信息、调度信息、身份信息,在经济模型中还包括调度契约等。2)运行数据。针对每个调度在实际运行中产生的参数,存放在资源所在的节点中,是全球网络论坛提出用来描述资源使用情况的记录规范,

收稿日期:2009-07-24;修回日期:2009-09-08。

基金项目:教育部科学技术研究重点项目(208148);甘肃省科技攻关项目(2GS064-A52-035-03)。

作者简介:何延年(1979-),男,甘肃酒泉人,讲师,主要研究方向:网络计算; 马满福(1968-),男,甘肃甘谷人,副教授,博士,主要研究方向:计算机系统结构、移动计算; 李勇(1979-),男,甘肃庆阳人,讲师,主要研究方向:网络计算; 曲伟丽(1984-),女,甘肃平凉人,硕士,主要研究方向:网络计算。

用资源使用记录(Resource Usage Record, RUR)<sup>[7]</sup>来描述,它通过GMA获取。3)网络数据。网络数据是反映网格底层网络随时间运行的参数,通过网络性能监测工具得到,如SPAND(Shared Passive Network Performance Discovery)等,数据存放在网络管理机构的MIB(Management Information Base)。在网格调度中,出现调度失败等现象时,可能是由于网络的拥塞导致的丢包等原因造成,而非资源本身所致,网络数据可帮助审计分析出现这些现象的原因,以便准确地评价资源。4)运行日志。日志从大的方面可划分为网格日志和网络日志两类,通过网格和网络基础设施获得。网格日志包含了非常丰富的动态数据,记录了资源和用户在网格中活动的行为,由此实现审计中随时间的分析;网络日志反映非网格调度中的实体行为数据,是网格日志的补充。

## 2 审计模型

具有审计系统的信任模型如图2所示。

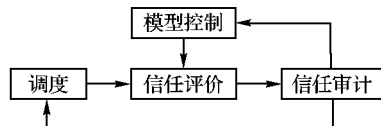


图2 具有审计功能的信任模型

用户按照任务实现提出的服务质量(Quality of Service, QoS)要求和调度所产生的行为结果进行比较,给出信任评价。信任审计则利用更为广泛和全面的数据,发现评价是否公正和准确,评价结果反馈给调度算法和评价模型,以策略的方式影响后续的调度和评价。

审计包括数据标准化、距离计算和异常评价发现等步骤。设服务质量参数定义为  $QoS = (q_1, q_2, \dots, q_n)$ , 用户  $u_i$  在时间周期  $T$  内的对所调用资源的信任评价为  $E = (e_1, e_2, \dots, e_m)$ , 其中第  $i$  个调度对应的 QoS 需求为  $QoS_{ib} = (q_{i,1}^b, q_{i,2}^b, \dots, q_{i,n}^b)$ ,  $i = 1, 2, \dots, m$ , 实际调度结束后的参数为  $QoS_{ie} = (q_{i,1}^e, q_{i,2}^e, \dots, q_{i,n}^e)$ 。对于被用户  $u_k$  调度过的资源  $r_l$ , 在时间  $T$  内对应的调用用户集合为  $U$ , 则针对每个调度,有如下处理:

### 2.1 数据标准化

不同的调度分别对应不同的 QoS 参数:一方面,用户任务的需求不同;另一方面,资源性能和完成情况不同。因此,  $QoS_{ib}$  和  $QoS_{ie}$  对于不同调度,不具有直接可比性。为了建立它们之间的有一致含义的参数,在计算距离之前,将数据进行标准化。

用户的第  $i$  次对  $r_l$  的调度,令  $p_i$  表示在 QoS 上各个参数按照预期约定和实际完成的良好程度百分比,即  $p_i = (p_{i,1}, p_{i,2}, \dots, p_{i,n})$ , 对于  $p_{i,j} = \frac{(q_{i,j}^b - q_{i,j}^e)}{q_{i,j}^b}$ ,  $j = 1, 2, \dots, n$ 。逐一计算  $U$  中每个用户的  $p_i$ , 形成资源服务标准化质量矩阵  $A = p_{s,t}$ , 其中,  $s = 1, 2, \dots, n$ ;  $t = 1, 2, \dots, |U|$ 。设  $\bar{x}_s, R_s$  分别表示矩阵中第  $s$  个值的均值、标准差,即:

$$\bar{x}_s = \frac{1}{|U|} \sum_{i=1}^{|U|} p_{i,s}$$

$$R_s = \frac{1}{|U|} \sum_{i=1}^{|U|} |p_{i,s} - \bar{x}_s|$$

则标准化后的数据为:

$$p_{s,t}^* = \frac{p_{s,t} - \bar{x}_s}{R_s}$$

### 2.2 距离计算

对于距离的计算,最常用的距离是曼哈顿距离和欧氏距离,这里采用欧氏距离:

$$d_{i,j} = \sqrt{\sum_{k=1}^n (p_{i,k}^* - p_{j,k}^*)^2}$$

在得到距离后,累计每个标准化数据与其他标准化数据的距离,形成距离矩阵  $R$ 。

### 2.3 异常评价发现

设  $D_i = \sum_{j=1}^n d_{i,j}$ ,  $D_i$  为矩阵  $R$  中第  $i$  行的距离之和, 其值越大,说明对应的评价距离其他评价越远,可能形成数据上的孤立点。计算矩阵的平均值  $\bar{D} = \frac{1}{|U|} \sum_{i=1}^{|U|} D_i$ , 然后比较  $D_i$  与  $\bar{D}$ , 定义异常评价为:如果  $D_i > 2\bar{D}$ , 则  $i$  为孤立点,即异常评价。

经过上述过程的计算,可以判定用户  $u_k$  在时间周期  $T$  内的对资源  $r_l$  的评价  $e_i$  是否异常,采用相同的过程,逐一评价并发现  $E = (e_1, e_2, \dots, e_m)$  中所有评价是否异常,得到审计结论  $AU = (au_1, au_2, \dots, au_m)$ , 其中  $au_i$  ( $i = 1, 2, \dots, m$ ) 取值为 0 或 1:0 表示评价无异常;1 表示评价异常。

### 2.4 评价结论及修正策略

主观评价受到用户环境和状态等个人不确定因素的影响,因此,一个审计周期内个别或者少数的异常评价是客观存在的,不需要处理。但是,当异常评价出现频繁或者较多时,则反映出该用户在评价上的习惯、偏好或者是恶意的评价问题,称为偏差评价用户,由此导致对调用资源的评价偏差是不允许的,需要纠正。在  $AU$  中,异常评价所占的比例为  $ab = \frac{\sum_{i=1}^m au_i}{|AU|}$ , 当  $ab > \alpha$ ,  $\alpha \in (0, 1)$  时,可认定为偏差评价用户。

对于异常评价,在线系统处理时可采用删除和修正两种策略,而审计系统是离线处理,因此无法删除,但可以通过模型控制对其加以修正。由于距离计算仅仅反映出一个评价偏离均值的程度,而不反映是偏高还是偏低,因此重新按照标准差  $R_s$  的计算公式,除去绝对值得  $R_{sin} = \frac{1}{|U|} \sum_{i=1}^{|U|} (p_{i,s} - \bar{x}_s)$  进行计算,如果所得的  $R_{sin} > 0$ , 则评价偏高;  $R_{sin} < 0$  时则偏低。由于评价偏离值为  $D_i - \bar{D}$ , 但该值的物理含义是用户评价的均值,且并不是该用户的所有评价均异常,因此不能完全按照该值进行修正。同时,修正必须保持原先用户评价的意图和含义,即不能将低的评价修正为高或者高的修正为低,因此修正只需将异常评价按照偏离程度修改为正常评价即可,即修改幅度为  $D_i - 2\bar{D}$ :

当  $R_{sin} > 0$ , 且  $D_i > 2\bar{D}$  时,对异常评价值进行  $e_i - (D_i - 2\bar{D})$  操作;当  $R_{sin} < 0$ , 且  $D_i > 2\bar{D}$  时,对异常评价值进行  $e_i + (D_i - 2\bar{D})$  操作。

### 2.5 审计周期

审计周期一方面应当动态地反映当前评价的准确性并加以修正;另一方面,审计过程是一个负载较大的计算过程,应以不过分增加系统负载为前提。系统状态的变化取决于系统中负载的变化规律和用户使用系统的习惯,审计周期首先应当和系统负载周期同步,并安排在系统轻载时进行。设系统

负载周期为  $T$ , 则审计周期按  $nT$  进行,  $n = 1, 2, 3, \dots$ , 一般地,  $n > 5$  为宜。

### 3 审计算法

用户  $u_k$  在审计周期  $T$  结束后, 进行数据采集和整合: 从部署在网格管理域的基础设施上获取调度契约, 读取服务质量的约定以及契约履行后的实际数据; 从信任管理机构获取该用户在该周期内的所有信任评价; 逐个按照所调度的资源, 读取对应资源在该周期内的调用者的全部信任评价。形成如下数据: 用户  $u_k$  的评价数组  $E = (e_1, e_2, \dots, e_m)$ , 所完成调度的质量需求矩阵  $QoS_{ib} = (q_{i,1}^b, q_{i,2}^b, \dots, q_{i,n}^b)$ , 实际完成的质量矩阵  $QoS_{ie} = (q_{i,1}^e, q_{i,2}^e, \dots, q_{i,n}^e)$ , 评价数组  $E$  对应的资源集合  $S_r = \{r_1, r_2, \dots, r_w\}$ , 其中  $w \leq m$  (同一资源可能被多次调用), 每个资源在  $T$  内的评价数组  $E_r = (e_1^r, e_2^r, \dots, e_q^r)$ , 其中  $q$  为正整数, 设待审计的用户集合为  $U_{audit}$ 。

算法分为三个步骤: 1) 初始化; 2) 针对每个用户所调度的所有资源, 进行评价过程; 3) 根据结果影响评价策略。算法伪代码如下:

```

Audit-as-Users(  $U_{audit}, \alpha$  );
1) Array  $AU[1 \dots m] = 0$ ;  $ab = 0$ ; // 初始化
   { For every  $u_k \in U_{audit}$  do
     For every  $r_i \in S_r$  do }
2) { calculate  $A = p_{s,t}$ ; //  $s = 1, 2, \dots, n; t = 1, 2, \dots, |U|$ 
      $\bar{x}_s = \frac{1}{|U|} \sum_{i=1}^{|U|} p_{i,t}$ ;
      $R_s = \frac{1}{|U|} \sum_{i=1}^{|U|} |p_{i,t} - \bar{x}_s|$ ;
      $p_{s,t}^* = \frac{p_{s,t} - \bar{x}_s}{R_s}$ ; // 标准化数据
      $d_{i,j} = \sqrt{\sum_{k=1}^n (p_{i,k}^* - p_{j,k}^*)^2}$ ; // 计算距离矩阵  $R$ 
      $\bar{D} = \frac{1}{|U|} \sum_{i=1}^{|U|} D_i$ ;  $D_i = \sum_{j=1}^n d_{i,j}$ ; // 矩阵的平均值
     If  $D_i > 2\bar{D}$  then
        $AU[i] = 1$ ; // 审计完成一个调度评价
3) For  $i = 1$  to  $q$  do  $ab = ab + AU[i]$  // 统计审计结果
   If  $ab/q > \alpha$  then
     modify(  $u_k$  )
   // 非正常评价习惯或恶意评价用户, 执行修正策略

```

## 4 实验分析

### 4.1 信任模型和调度算法

实验中采用 Farag Azzedin 等提出的声誉模型的计算方法<sup>[8]</sup>为补充的主观模型。令  $x$  为用户,  $y$  为资源, 在调度之前, 如果有对应的信任评价, 则以该评价为依据; 否则, 利用 Farag Azzedin 提出的方法进行声誉计算, 为初次调度提供信任依据。每次调度结束,  $x$  对  $y$  的服务提出信任评价。调度算法同样采用文献[8]提出的 TMA (Trust-aware Min-min Algorithm) 算法。

### 4.2 实验设计

原型系统以 GRACE (GRid Architecture for Computational Economy)<sup>[9]</sup>为平台进行构造, 系统由 40 个节点组成, 包括资源提供节点、信任模型管理和控制节点、审计节点、调度中的契约管理节点和资源的注册、发布以及部署 GRIS (Grid Resource Information Service) 等。系统中提供 5 类资源, 节点

既是资源的提供者, 也是任务的宿主者。在各个节点上, 任务采用符合泊松分布的随机函数进行调度以及资源的登录和退出, 为了取得更多的数据, 控制调度在高频率范围进行。实验中的任务平均执行周期为 50 ms, 审计周期为 30 min, 认定偏差评价用户的阈值  $\alpha$  取值分别为 0.2 和 0.4。为了发现审计对信任模型的影响, 实验中将 30% 的评价定义为恶意评价, 即评价直接给予一个区间  $[0, 1]$  的随机数, 而非按照实际任务完成情况进行。实验中, 一个审计周期内, 将信任值大于平均值的资源称为可信资源。

### 4.3 结果分析

实验分为审计和不审计两种情况进行, 从相同的初始状态开始, 系统运行一段较长时间并在第一个审计周期结束后开始采集数据。实验在系统吞吐量、可信任资源调度率、审计修正率和信任评价稳定性等参数上取得了实验结果, 完成了 8 个审计周期, 其参数的平均值见表 1、2 所示。

表 1  $\alpha = 0.2$  时的实验结果 (审计周期为 30 min)

算法	吞吐量	调度 失败率/%	可信资源 调度率/%	审计 修正率/%
TMA	128 526	8.71	63.60	-
有审计 TMA	146 917	3.87	72.32	4.15

从表 1 看出, 与非审计调度相比, 有审计的信任调度算法取得了较大的吞吐量, 比前者提高了 12.52%; 调度失败率则从 8.71% 降到 3.87%; 可信资源调度率从 63.60% 提高到 72.32%, 提高了 8.72 个百分点; 审计中有 4.15% 的恶意评价或非正规评价用户被修正。显然, 审计修正一定程度上避免了良好资源被恶意评价而导致的调度率下降问题, 使得系统维持了一个较高的资源任务匹配率, 因此吞吐量有所提高; 通过审计促使更多的资源按照其实际服务水平得到评价, 从而任务可按需求获得更优的资源, 调度失败率下降, 可信资源的调度率提高; 8 个周期的审计发现并修正了部分非正常评价用户的评价, 通过审计的可靠性控制是有效的。

表 2  $\alpha = 0.4$  时的实验结果 (审计周期为 30 min)

算法	吞吐量	调度 失败率/%	可信资源 调度率/%	审计 修正率/%
TMA	123 946	9.01	61.42	-
有审计 TMA	138 674	5.82	67.57	1.75

表 2 显示, 由于偏差评价阈值  $\alpha$  的增大, 一定程度上放宽了对用户评价的要求, 与  $\alpha = 0.2$  相比, 审计修正率下降到 1.75%; 吞吐量和可信资源调度率也下有所下降, 而调度失败率从 3.87% 提高到 5.82%。由此看出, 在实验中存在 30% 恶意评价的情况下,  $\alpha = 0.4$  的取值不是合适的, 仍然放任了恶意评价的存在, 影响系统效率的提高。从理论上分析,  $\alpha$  是一个经验值, 其大小应当与系统中存在的恶意评价用户所占的比例相当。

从图 3 看出, 没有审计的信任调度中, 由于存在大量的恶意评价, 全部资源的信任评价均值随时间呈下降趋势。尽管恶意评价也会给出高的评价, 但该高值在正常评价的调度中由于资源的服务质量与事实不符, 导致在正常评价中给予较低的值, 造成总体趋势下降。而带有审计并通过其修正评价模型的, 信任则随时间呈现上升趋势。可见, 在尽可能去除了恶意评价后, 总体评价呈稳定状态。其原因在于, 减少了随意评价的干扰后, 使得资源按照实际的服务水平与任务需

求进行匹配,降低了因信任度夸大导致调度失败和信任度减小导致的资源空闲。

从实验结果和分析看出,对用户信任评价的审计是有效的,它发现了评价中存在的问题,而审计结果驱动信任评价模型则抑制了随意评价,将其影响适当消除,提高并保证了信任的有序以及公正,由此维护了评价模型的稳定性,进而促进了系统的稳定性和有效性。审计有较大的计算复杂度,实验中采用独立节点进行数据采集和审计,因此未涉及对系统的负载影响评价。按照实际运行中的网格环境,审计可在系统空闲时间进行,对系统的正常调度不造成过分负担。

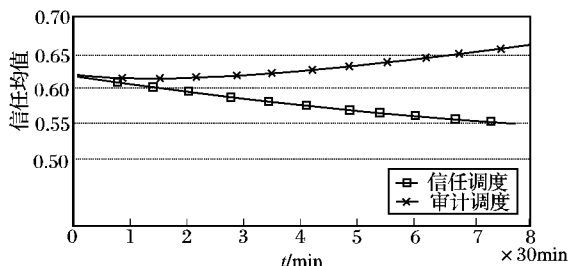


图3 信任均值随时间变化趋势

## 5 结语

文文利用网格环境下各类数据的支撑,对用户进行的信任评价进行审计,从两个方面取得了进展:1)将审计的概念引入信任模型;2)将审计结果作用于信任模型的修正。实验表明,所提出的方法在存在大量随意评价的情况下,保持了信任模型的稳定性,进而维护了整个系统的稳定性,是有效的。

### 参考文献:

[1] YU BIN, SINGH M P. Detecting deception in reputation management[C]// Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems. New York: ACM, 2003: 14-18.

[2] SEHULTER A, REIS J A, KOCH F. A grid-based intrusion detection system[C]// Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies. Washington, DC: IEEE Computer Society, 2006: 187-187.

[3] BAHARINK N B, DINN M K, JAMALUDIN M Z, *et al.* Third party security audit procedure for network environment[C]// Proceedings of 4th National Conference on Telecommunication Technology. New York: IEEE, 2003: 26-30.

[4] TIERNEY B, AYDT R, GUNTER D, *et al.* A grid monitoring architecture[EB/OL]. [2009-03-20]. <http://www.didc.lbl.gov/GGF-PERF/GMA-WG/papers/GWD-GP-16-1.pdf>.

[5] NI GUANGBAO, MA JIE, LI BO. GridView: A dynamic and visual grid monitoring system[C]// Proceedings of the 7th International Conference on High Performance Computing and Grid in Asia Pacific Region. New York: IEEE, 2004: 89-92.

[6] VARALAKSHMI P, SELVI S T, KANCHANA P, *et al.* A robust trust model with rated-genuine feedbacks in a grid environment[C]// Proceedings of International Conference on Computational Intelligence and Multimedia Applications. Washington, DC: IEEE Computer Society, 2007: 412-419.

[7] Global Grid Forum. RUR: Resource Usage Record Working Group[EB/OL]. [2009-02-20]. [http://www.gridforum.org/3\\_SRM/](http://www.gridforum.org/3_SRM/)

[8] AZEDIN F, MAHESWARAN M. Integrating trust into grid resource management systems[C]// Proceedings of International Conference on Parallel Processing. Washington, DC: IEEE Computer Society, 2002: 47-54.

[9] BUYYA R, ABRAMSON D, GIDDY J. Nimrod/G: An architecture for a resource management and scheduling system in a global computational grid[C]// Proceedings of the 4th International Conference on High Performance Computing in the Asia-Pacific Region. Washington, DC: IEEE Computer Society, 2000: 283-289.

(上接第254页)

选用不同数量的传感器读数作为特征向量,定义测试点 $(x', y')$ 和实际位置 $(x, y)$ 满足 $|x' - x| \leq 2$ 且 $|y' - y| \leq 2$ 为准确,对所有的测试集中的数据进行测试。准确率为所有测试点中结果准确的比例,选用不同数量的传感器读数作为特征向量时准确率如表2所示。

表1 条件概率方法的ECDF实验结果

$(x, y)$	$(R_1, R_5, R_7, R_8)$	$(x', y')$
(2, 1)	(223, 227, 227, 231)	(2, 2)
(2, 3)	(222, 219, 216, 214)	(3, 3)
(5, 7)	(219, 225, 224, 224)	(5, 8)
(7, 7)	(214, 235, 227, 229)	(7, 8)
(9, 1)	(212, 222, 216, 221)	(10, 2)
(9, 3)	(219, 224, 221, 223)	(10, 4)

表2 电子地图方法的ECDF实验结果

锚节点编号	准确率/%
1, 5, 7, 8	97.33
2, 5, 8	89.33
5, 7, 8	86.67

## 3 结语

本文针对智能建筑中的目标分布问题,使用与无线传感

器网络融合的方法,提出ECDF方法,利用条件密度和电子地图的方法对目标分布进行判断。实验结果表明,这种方法都能够有效地判断目标的分布,准确性高,鲁棒性好。在此基础上,使用电子地图的方法在清华大学建筑节能楼二层会议室内实现了无线传感器与照明系统集成。集成之后的照明系统可以根据室内人员的分布情况调节照明灯光的明暗,亮灭,有效地节约了照明用电。可以预见,无线传感器网络将在智能楼宇中有更加广泛的应用。

### 参考文献:

[1] 夏俐,陈曦,赵千川,等. 无线传感器网络及其应用简介[J]. 自动化博览, 2004, 21(1): 33-35.

[2] 李建中,高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展, 2008, 45(1): 1-15.

[3] 梁文华,刘庆. 智能建筑系统集成设计之综述[J]. 计算机应用与软件, 2008, 24(4): 182-183.

[4] 朱炜. 智能建筑弱电综合布线系统综述[J]. 计算机时代, 2006(5): 46-48.

[5] TARN J, CHANG W, HSU B. Three-dimensional modeling of 900-MHz and 2.44-GHz radio propagation in corridors[J]. IEEE Transactions on Vehicular Technology, 1997, 46(2): 519-527.

[6] KARL H, WILLIG A. Protocols and architectures for wireless sensor networks[M]. Hoboken, NJ: John Wiley and Sons, 2005.