文章编号:1001-9081(2007)01-0128-04

一种基于克隆网络聚类的入侵检测方法

张 喆[1],白 琳[2]
(1. 兰州理工大学 计算机与通信学院,甘肃 兰州 730000;
2. 西安邮电学院 信息中心,陕西 西安 710061)
(zzeboy1980@yahoo.com.cn)

摘 要:将免疫克隆策略用于网络结构的聚类中,能够得到克隆网络对数据进行合理的聚类分析。采用克隆网络对入侵检测数据进行学习,即用一个小规模网络来表示海量数据,完成数据的压缩表示。再利用图论中的最小生成树对克隆网络的结构进行聚类分析,从而获得描述正常行为和异常行为的数据特征,实现合理的聚类。该算法可实现对大规模无标识原始数据的入侵检测,区分正常和异常行为,并能检测到未知攻击。在 KDD CUP99数据集中进行了对比仿真实验,实验结果表明:相对于以前的算法,该算法较大地提高了对已知攻击和未知攻击的入侵检测率,并降低了误警率。

关键词:免疫克隆策略;克隆网络;无监督聚类;入侵检测
中图分类号: TP309 **文献标识码**: A

Intrusion detection method based on clonal network clustering

ZHANG Zhe[1], BAI Lin[2]
(1. School of Computer and Communications, Lanzhou University of Technology, Lanzhou Gansu 730000, China;
2. Center of Network Information, Xi'an Institute of Post and Telecommunications, Xi'an Shaanxi 710061, China)

Abstract: Reasonable clustering analysis of data done by clonal network can be obtained when the strategy of immunity cloning is applied to network clustering. By expressing the magnanimity datum with a small-scale network, clonal network structure was adopted in training the intrusion detection so as to get the compressed data. What's more, the Minimal Spanning Tree in the term of Graph Theory was employed to perform clustering analysis on network structure and achieve the characterization of normal and abnormal data finally. This clustering algorithm can deal with network intrusion detection from mass unlabeled data, distinguish between normal and abnormal data and detect unknown attacks. The computer simulations on the KDD CUP99 dataset show that this algorithm can achieve higher detection rate of known or unknown attacks and lower false positive rate when compared with the previous algorithms.

Key words: immunity clonal strategy; clonal network; unsupervised clustering; intrusion detection

0 引言

入侵检测技术包括误用检测和异常检测[1]。误用检测建立攻击行为特征库,采用特征匹配的方法确定攻击事件;异常检测建立用户正常行为模型,以是否显著偏离正常模型为依据进行检测,能够发现新的攻击类型。

传统入侵检测系统对未知攻击的检测能力很有限。大多数检测系统采用有监督的学习算法[2],需要大量带标签或完全正常的数据来训练获得正常模型,如果训练数据的标签错误,会影响算法的有效性。况且要为系统的学习收集大量带标签的数据或完全正常的数据是不易实现的。所以,新型的入侵检测系统应该采用无监督学习算法并具备检测未知攻击的能力。

聚类分析的任务是把一个未标记的样本集按某种准则划分成若干子集,将相似的样本尽量归为一类,不相似的样本归为不同类。这种方法可以定量地确定研究对象之间的亲疏关系,达到合理的分类。

一些聚类算法已被用于入侵检测中[3~5],文献[3]提出免疫 C均值聚类入侵检测系统,该算法依赖先验知识并对初始化敏感。文献[4,5]采用简单的基于距离的聚类算法,虽属无监督聚类,但需要预先设定重要参数,由于没有合适的方法设定参数值,只能用试探法人为干预,必然影响系统的性能。

Leandro在 2000年提出进化人工免疫网络(Evolutionary Artificial Immune Network, AiNet)[6]并将其用于聚类来解决聚类前需要类数以及原型类型先验知识的问题。但 AiNet对类间边界不清晰的数据集无能为力。

克隆算法[7]将进化搜索与随机搜索、全局搜索和局部搜索相结合,能以概率 1收敛到全局最优解。将免疫克隆策略用于网络结构聚类,并将克隆选择和禁忌克隆结合,得到的克隆网络兼具免疫特异性和免疫耐受性,能够克服边界不清晰对聚类效果的影响。本文将这种克隆网络聚类算法用于入侵检测。首先用训练数据来"进化"一个克隆网络,使网络结构反映原始数据的分布情况;然后利用图论中的最小生成树对网络结构进行聚类分析,最终获得描述正常行为和异常行为的数据特征。

1 人工免疫系统

1.1 免疫克隆算法

免疫克隆算法包括三个步骤:克隆操作、免疫基因操作和

收稿日期:2006-07-05;**修订日期**:2006-10-12 **基金项目**:甘肃省自然科学基金资助项目(3ZS051-A25-037);陕西省中青年科研基金资助项目(109-0206);西安邮电学院中青年科研基金资助项目(302-0405)

作者简介:张喆(1980-),男,河北唐山人,硕士研究生,主要研究方向:计算方法、网络行为分析; 白琳(1980-),女,陕西商州人,讲师,硕士研究生,主要研究方向:计算智能、信息处理。

克隆选择操作。克隆的实质就是在进化过程中,在每一代最优解的附近,根据亲和度的大小进行克隆,产生一个变异解的群体,增加抗体的多样性,从而扩大了搜索范围。将一个低维空间(n维)的问题转化到更高维(N维)的空间中解决,然后将结果投影到低维空间(n维)中,从而获得对问题更全面的认识。[8]

1.2 进化人工免疫网络

Leandro根据 Jeme的独特型网络学说[9]理论,提出一种进化人工免疫网络(AiNet)。其主要思想是:设 $X = \{x_1, x_2, \cdots, x_n\}$是待聚类的对象的全体(论域),其中 $x_i = (x_{i1}, x_{i2}, \cdots, x_{ip})^T$表示第 i个样本的 p个特征值,$x_i$可用状态空间 S^m中的一个点 s来表示,将 s作为抗原,来决定抗体-抗体(Ab-Ab)以及抗原-抗体(Ag-Ab)之间的相互作用。并且系统内部的相互作用可以用一个连通图来表示。

网络模型定义为:人工免疫网络是一个加权的图 G,该图由一组不完全连接的神经元节点构成,每对节点产生一条边,边的长度称为权值或者连接强度。

1.3 克隆网络

为了解决免疫网络对边界模糊的数据集不能有效分类的问题,文献[10]提出禁忌克隆的概念,将克隆算子和禁忌克隆结合,构造克隆网络对数据有效聚类。

根据免疫网络理论,当机体内出现一个新的抗原时,现有抗体(网络节点)要对其进行识别,成功识别的抗体将激活网络,并导致相应抗体增殖。若该抗原对应为噪声点或处于不明显边界上的样本点,则进行禁忌克隆操作,将相应的抗体排除。禁忌克隆可以使网络产生免疫耐受性,解决边界模糊数据集的聚类问题。

2 基于克隆网络聚类的入侵检测算法

由聚类的目标函数 C(W, P)知,聚类的目的就是要获得数据集 X的模糊划分矩阵 W和聚类原型 P。W和 P是相关的,那么已知其一即可求得另一个的解,我们令一组聚类原型 P就是一个抗体。根据目标函数越小,则聚类效果越好,抗体-抗原亲和度越大的原则来构造抗原 x_i($i = 1, \cdots, n$)与抗体 y_j($j = 1, \cdots, m$)的亲和度函数 $f(x_i, y_j)$,$f(x_i, y_j)$越大,说明 y_j越接近 x_i。

抗体-抗体亲和度 s_{ij}等于它们的距离测度,即 $s_{ij} = d(y_i, y_j)$。s_{ij}越小,y_i与 y_j差异越小,抗体间亲和度越大。

由于入侵检测数据包括连续属性和离散属性,而许多聚类算法在计算数据差异度时往往采用欧氏距离作为衡量标准,在处理入侵数据时,只考虑其数值属性值,而忽略非数值属性的信息。因此本文采用重新定义的混合型(离散的和连续的属性)数据差异度衡量标准来提高聚类精度。新的距离测度定义为:

$$d(x_i, x_j) = \sqrt{\sum_{k=c1}^{c_m} (x_{ik} - x_{jk})^2 + \lambda \sum_{l=d1}^{d_m} \delta(x_{il}, x_{jl})} \quad (1)$$

其中,根号中的第一项是连续属性的欧几里得距离的平方,第二项是离散属性的相异匹配测度,常数 λ用来调节两种属性在目标函数中的比例。δ(·)定义为:

$$\delta(x, y) = \begin{cases} 0, & x = y \\ 1, & x \neq y \end{cases}$$

2.1 克隆网络学习算法

算法步骤如下:1) $l = 1$,初始化抗体群 C:网络节点即抗体 y_j($j = 1, 2, \cdots, N_c$)是 N_c个 p维向量;

2)对每个抗原 x_i($i = 1, 2, \cdots, n$),进行如下操作:

2.1)计算抗原-抗体的亲和度:

$$f(x_i, y_i) = \frac{1}{1 + (x_i - y_j)^T (x_i - y_j)} \quad (2)$$

2.2)选择 k个亲和度最高的抗体($y_{r1}, y_{r2}, \cdots, y_{rk}$),按亲和度越高,克隆规模越大的原则进行抗体的 q_m克隆:

$$T_c^C(y_m) = I_m \times y_m, \quad m = 1, 2, \cdots, k \quad (3)$$

其中 I_m为元素为 1的 q_m维行向量。

$$q_m = \mathrm{Int}\left[n_c \times \frac{f(x_i, y_m)}{\sum_{h=1}^{k} f(x_i, y_m)} \right], \quad m = 1, \cdots, k \quad (4)$$

Int(x)表示大于 x的最小整数,n_c为设定的克隆总规模,本文实际值为 $n_c^* = \sum_{m=1}^{k} q_m$;

2.3)变异:对克隆后的抗体 y_j^*变异操作,提高克隆节点与 x_i的亲和度:

$$C = C - \alpha(C - X) \quad (5)$$

α为变异概率,根据亲和度越高,变异概率越小的原则,本文令 $\alpha = 1 - f(y_j^*, x_i)$;

2.4)计算抗体-抗原亲和度,选取 l% 亲和度最高抗体组成记忆单元,得到矩阵 M_p。

2.5)删除 M_p中节点亲和度小于亲和度门限 σ_d的神经元来减小矩阵规模;

2.6)计算 M_p中抗体间亲和力 $s'_{ij} = \| y_i^* - y_j^* \|$,将 s'_{ij}小于压缩门限 σ_s的抗体死亡;

2.7)将记忆细胞 M_p加入原始抗体 C:$C \leftarrow [C; M_p]$;

3)禁忌克隆:计算每个抗体和其他抗体的亲和力,若亲和力小于门限 σ_s的抗体个数小于 σ_f,将该抗体删除;

4)计算 C中抗体-抗体亲和力 s_{ij},将 s_{ij}小于 σ_s的抗体死亡,选取若干抗体代替删除的抗体加入 C中;

5) $l = l + 1$,若满足终止条件(迭代到预先设定次数),转 6),否则返回 2);

6)网络输出,算法停止。

该算法包括抗体-抗原识别、免疫克隆增殖、亲和度成熟以及网络抑制。算法中存在两个压缩步骤:克隆压缩和网络压缩。网络的输出是由代表抗原网络内部图像的记忆矩阵和决定网络节点间相互联系并描述网络结构的内部亲合矩阵组成。

在第 2.6步中的压缩门限 σ_s控制着网络节点间的亲合程度。它通过调整抗体细胞的特异性水平来控制网络的可塑性和聚类精度,对聚类的结果和性能影响很大,通常先设定一较小值($\sigma_s \leqslant 10^{-3}$),再根据实验结果不断增加,最终确定一个合适的参数。本文经测试,取 0.25。

本文算法对亲和度高的个体克隆操作,将全局和局部搜索结合,避免陷入局部极值的问题;第 2.6步和第 4步通过克隆死亡和网络压缩来控制网络规模。第 3步通过禁忌克隆操作使网络产生免疫耐受性。这样将克隆选择和禁忌克隆结合,使网络兼局免疫特异性和免疫耐受性。同时,算法在每代个体中进行变异和克隆选择,使网络的动态性能和结构受进化策略控制。所以克隆网络具有自学习、自适应能力,能够发现数据集中的结构分布。为了确定数据集的聚类结构及每个样本点所属类别,本文采用最小生成树[10]来实现。

2.2 最小生成树(MST)

连通图的最小生成树是寻找网络节点内部联系的有力工

具,能够描述网络结构的聚类。它定义为:连通图 G的一个子图如果是一棵包含 G所有节点的树,该子图就是 G的生成树;使各边权值之和最小的生成树是 G的最小生成树。

得到了网络结构的最小生成树后,用条形(Bar)图描述MST的边长,通过从 MST中删除某条边(如果 MST中某条边的权值明显大于其近邻边的权值就将其删除)的操作产生该MST的子树集,每个子树为一个聚类。Bar图中山谷的数目就是数据集的聚类类别数。

2.3 聚类类别标定

利用克隆网络和 MST对训练数据进行聚类分析,得到聚类原型。数据集被划分为 h个子集,每个子集 $P_c(1\leqslant c\leqslant h)$中包含属于该子集的所有抗体。每个子集内部的元素互相接近,与其他子集中的元素则相对较远。

我们给每个子集一个唯一的标签将其标记。对数据集 $X=\{x_1,\cdots,x_n\}$,计算 $x_i(1\leqslant i\leqslant n)$和各子集的距离,找到最短距离 $d(x_i,P_m)(1\leqslant m\leqslant h)$,则第 m个子集的标签就是 x_i所属的类别。这样即可完成对训练数据的分类。

在入侵检测系统中,需要对各子集标定类别,确定正常类和异常类。检测系统基于两个合理的假设[5]:同类数据在合理的尺度条件下在特征空间中互相接近,不同类数据彼此远离;入侵行为和正常行为本质特性差异很大且相对很少,这在实际中是合理的。因此,根据样本分布,子类中数据量就可以划分各个正常类和异常类。如果某类的数据量与样本数据总量之比不小于 $r(0<r<1)$,将其标记为正常。当然,如果加入专家知识,可以把异常类细分,确定每个异常类是何种攻击类型。

2.4 检测算法

对应于正常类的抗体是正常数据代表点,即正常模型。根据正常和异常模型即可进行入侵检测。对于数据集 $Y=\{y_1,\cdots,y_n\}$,计算 $y_i(1\leqslant i\leqslant n)$和各原型 p_j的距离,找到最短距离 $d(x_i,p_m)(1\leqslant m\leqslant N_C)$。那么 p_m就是 y_i的代表点。根据 p_m所属模型的类别(正常或异常)可确定 y_i是否异常。若 $d(x_i,p_m)\geqslant\eta$,应判断 y_i为未知攻击。

3 仿真实验与结果分析

3.1 数据预处理

本文实验采用 KDD CUP99[11]标准数据集,该数据集共计 4 900 000多条连接记录,包含 9个星期的网络流量,其中 7周时间的训练数据包含约 500万条连接记录,2周时间的测试数据约包含 200万条连接记录。每条记录都带有持续时间、协议类型等参数,参数属性共计 42个,其中 8个是离散属性,33个是连续属性。

KDD CUP99数据集包含 4大类攻击。在 KDD CUP99的训练数据中,共有 23个不同的连接标志,除"正常"外,其余22个代表攻击类型,这些攻击可以分成如前所述的四类攻击模式。测试集中共包含 38个不同的连接标志,除"正常"外,其余 37种代表攻击类型。在 37种攻击类型种,有 15种未在训练集中出现,对训练数据而言是新的攻击模式,我们称其为未知攻击。

数据预处理时,我们先将字符枚举特征变成离散数值特征,用不同的自然数代表不同的字符枚举型属性值。例如,用1表示"http"协议,2表示"ftp"协议。

考虑到入侵数据的多个属性的度量单位不同会影响聚类的结果,需要对数据的连续属性归一化来保证各属性在同一个区间内取值,防止由于特征属性数量级差别较大而造成某些属性占主导地位使得数量小的属性特征无法发挥作用。归一化的方法为:

计算平均的绝对误差:

$$s_f=\frac{1}{N}\sum_{i=1}^{n}(x_{if}-m_f) \tag{6}$$

其中:$x_{1f},\cdots,x_{nf}$是 f的 n个属性,m_f是 f的平均值:

$$m_f=\frac{1}{N}\sum_{i=1}^{n}X_{if}$$

计算标准化的特征属性值:

$$Z_{if}=\frac{x_{if}-m_f}{s_f} \tag{7}$$

3.2 实验结果

因原始数据量过于庞大,本文从 KDD CUP9910%训练集中随机选取 20万条记录作为训练样本,其中入侵记录2 200条(包含 22种攻击类型)。如上所述,对训练集而言,存在 15种未知攻击类型。为了测试算法对未知攻击的检测效果,从KDD CUP99测试数据集中各选取 10万条数据作为两个测试集,其中入侵数据为 1 000条(包含未知攻击和已知攻击类型在内的 37种攻击类型)。

训练数据经过聚类分析,产生克隆网络,网络中有 p个抗体。采用 MST对网络结构进行分析,得到聚类类别数 c,当 c值较大,说明算法将某个正常或异常类细分为 n小类,那么可以依据某一准则将这 n个小类合并来确定最终聚类结果,得到代表正常行为和异常行为的模型。

表 1 三种算法所得各类间距离

算法	类别	2	3	4	5	6	7
本文算法	1	12.78	19.35	21.33	19.13	—	—
	2	—	25.12	17.98	19.38	—	—
	3	—	—	16.55	17.19	—	—
	4	—	—	—	19.06	—	—
文献[3]算法	1	12.33	15.35	15.97	15.87	12.95	13.88
	2	—	15.07	16.75	18.87	13.34	10.03
	3	—	—	11.76	14.46	12.35	13.14
	4	—	—	—	10.89	11.12	16.15
	5	—	—	—	—	11.23	15.93
	6	—	—	—	—	—	15.02
文献[4]算法	1	12.31	18.63	18.86	13.22	15.28	—
	2	—	15.87	17.15	16.56	15.88	—
	3	—	—	11.62	15.31	13.17	—
	4	—	—	—	17.23	17.78	—
	5	—	—	—	—	14.25	—

本文将文献[3]和文献[4]算法作为比较算法。经过 30次独立实验,在平均的情况下,本文算法通过对训练数据集的分析得到 5个子集,文献[3]和文献[4]算法聚类类数分别为7和 6。聚类结果见表 1和表 2。对于聚类结果,类间距大,类内距离小,算法的性能就高[12]。

表 2 三种算法所得各类内距离

类别	1	2	3	4	5	6	7
本文算法	1.27	1.58	1.33	1.15	2.26	—	—
文献[3]算法	2.88	2.05	3.33	3.81	4.46	2.05	2.39
文献[4]算法	1.87	2.38	2.75	3.83	4.07	3.22	—

说明:由于采用三种算法得到的类数不同,在表 1、表 2中,符号"—"表示两类之间的距离为 0或由于不存在的类而导致相应类间距或类内距空缺。

类内距定义为:

$$D_c = \frac{1}{n(n-1)} \sum_{i=1}^{n} \sum_{j=1}^{n} d(x_i, x_j),\ c \in [1, r] \quad (8)$$

其中 r为聚类数。

类间距定义为:

$$D(c_i, c_j) = \frac{1}{n_i n_j} \sum_{p \in c_i} \sum_{q \in c_j} d(p, q) \quad (9)$$

其中 n为各类所含对象数。

根据 2.3节的类别标定原则,对本文算法的聚类结果,可确定 1个正常类(类 1)。文献[3]和文献[4]算法分别有 3个(类 1、6、7)和 2个(类 1、2)正常类。

入侵检测相关统计量定义为:检测率指被检测出的异常样本数占异常样本总数的百分比。误警率指正常样本被识别成异常样本的数目占正常样本总数的百分比。

通过聚类得到正常模型对测试集进行检测。本文算法将训练集分为 6类,根据 3.3节的检测过程,对于某测试数据,当它属于第 1类时,就将其标为正常,否则,不管它属于何种攻击类,都将其作为异常数据来计算检测率(此数据应是被正确检测到的入侵数据);对于正常数据,无论将其误认到哪个攻击类中,都将其作为误警数据来计算误警率。表 3给出了三种算法经 20次独立实验的平均检测结果(已知入侵指训练样本中包含的 22种攻击;未知入侵指训练集中未包含的 15种攻击)。

表 3　三种算法检测结果

训练数据集	测试数据集	算法	已知入侵检测率	未知入侵检测率	误警率
样本总数 200000	test1 样本总数 100000 入侵数据 1000 条	本文算法	91.21%	84.00%	4.06%
		文献[3]算法	60.93%	49.66%	7.78%
		文献[4]算法	63.25%	51.12%	6.53%
入侵数据 2200 条	test2 样本总数 100000 入侵数据 1000 条	本文算法	92.05%	83.25%	3.97%
		文献[3]算法	61.33%	50.98%	7.55%
		文献[4]算法	65.01%	50.35%	6.85%

3.3　实验结果分析

从表 1、2可看出,本文聚类算法满足信息处理对聚类的典型要求[12]:

(1)不依赖先验知识,用于决定参数的领域知识较少;

(2)与数据分布无关,能够有效的逼近任意形状分布的样本集;

(3)对输入记录的顺序不敏感;

(4)能够处理不同类型的属性以及噪声数据;

(5)具有高维性、可伸缩性、可解释性和可用性,能够有效的处理大规模数据集。

从表 3可以看出,本文算法用于入侵检测,误警率和检测率都比其他算法理想。可见,基于克隆网络聚类的入侵检测系统是有效的。由于文献[4]的算法对每一类只保留一个点,而本文方法对每一类保留若干个点,所以本文算法能更好地逼近任意形状分布的数据,与数据分布无关,但计算速度不及文献[4]的方法。同时本文算法将免疫克隆策略和禁忌克隆操作结合,对边界不清晰的数据集分类有效,克隆网络聚类不仅能够处理海量、多维异构的数据,而且不依赖先验知识,收敛速度快,聚类性能好,使仿真实验具有更好的检测结果。

参考文献:

[1] 戴英侠,连一峰,王航. 系统安全与入侵检测[M]. 北京:清华大学出版社. 2002.

[2] 蒋建春,马恒太,任党恩. 网络安全入侵检测:研究综述[J]. 软件学报, 2000, 11(11): 1460－1466.

[3] 罗静, 刘芳. 一种基于免疫的模糊 C均值入侵检测方法[A]. 西安电子科技大学第二届研究生学术年会[C]. 2003.

[4] 罗敏,王丽娜,张焕国. 基于无监督聚类的入侵检测方法[J]. 电子学报, 2003, 11(11): 1714－1716.

[5] PORTNOY L. Intrusion Detection with Unlabeled Data using Clustering[D]. Columbia University, 2000.

[6] CASTRO LND, ZUBEN FJV. An evolutionary immune network for data clustering[A]. Proceedings of the Sixth Brazilian Symposium on Neural Networks[C]. 2000. 84－89.

[7] DU HF, JIAO LC, WANG SA. Clonal Operator and Antibody Clone Algorithms[A]. Proceedings of the First International Conference on Machine Learning and Cybernetics[C]2002. 506－510.

[8] 焦李成,杜海峰. 人工免疫系统进展与展望[J]. 电子学报, 2003, 31(10): 1540－1549.

[9] 杜海峰. 免疫克隆计算与人工免疫网络研究与应用[D]. 西安:西安电子科技大学, 2003.

[10] 李洁,高新波,焦李成. 基于克隆算法的网络结构聚类新算法[J]. 电子学报, 2004, 32(7): 1195－1199.

[11] kdd cup99 dataset[EB/OL]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html 1999－12－10.

[12] HAN JW, KAMBER M. 数据挖掘概念与技术[M]. 范明,孟小峰,译. 北京:机械工业出版社, 2001.

中国自动化学会第二十二届青年学术年会(YAC'2007)征文通知

中国自动化学会第二十二届青年学术年会(YAC'2007)将于 2007年 8月初在桂林召开。本次会议由中国自动化学会、中国自动化学会青年工作委员会举办,桂林空军学院承办。会议设有优秀论文奖和优秀应用论文奖,会议还将评选有一定成就和愿意为青年委员会工作的年青委员数名。热烈欢迎全国青年科技工作者及学生积极参加。

一、征文范围

(1)线性与非线性系统控制;(2)自适应控制和预测控制;(3)H∞控制和鲁棒控制;(4)智能控制、模糊控制;(5)系统辨识与建模;(6)故障诊断与容错控制;(7)神经网络及控制;(8)自动化仪表与过程控制;(9)软件工程、并行处理;(10)人工智能与专家系统;(11)计算机视觉、图像处理与模式识别;(12)机器人与机器人控制;(13)大系统;(14)电力系统及其自动化;(15)电机驱动及运动控制;(16)传感器与检测技术;(17)离散事件动态系统;(18)计算机集成制造系统;(19)计算机软硬件技术及其应用;(20)系统工程理论、方法及其应用;(21)自动化指挥系统;(22)数据融合与软测量;(23)单片机控制及应用技术;(24)火力指挥与控制系统;(25)企业改革、发展策略及管理决策;(26)工业过程控制与生产管理;(27)图书馆自动化与数字图书馆技术;(28)其他。

二、征文要求

(1)录用论文将以国家中文核心期刊专集或者由出版社出版论文集(《自动化理论、技术及应用》)等形式刊登出版;(2)论文应具有一定的学术或实用价值,未在国内外学术期刊或会议发表过;(3)论文第一作者的年龄不超过 45岁;(4)来稿中英文皆可,请用 Word 2000以上版本编排文稿,版面格式见《自动化学报》,A4纸打印,一式三份邮寄或用 E-mail发出(地址见文末);(5)投稿时请注明文章所属方向(见征文范围);(6)请注明联系作者的详细通讯地址、电话及 E-mail;(7)因版权或保密等引起的纠纷或责任,作者自负。

三、重要日期

截稿日期:2007年 5月 31日

录用日期:2007年 6月 30日以前发录用与否通知

四、投稿地址

541003

广西桂林空军学院火力与指挥控制系 YAC'2007组委会

倪国旗

电话:0773－2084109或 13977383512

E-mail: yac2007@163.com 或 yac2007@sina.com