

MVL 条件下 k-out-of-n: S 系统的研究^{*})

郑吉平^{1,2} 秦小麟^{1,2} 孙 瑾¹

(南京航空航天大学信息科学与技术学院 南京 210016)¹

(南京航空航天大学信息安全研究所 南京 210016)²

摘 要 复杂网络环境下的系统组件往往处于多种不同状态,二值逻辑(BL)在描述多种组件状态时显得无能为力。本文提出了采用多值逻辑(MVL)分析组件状态,重点描述 k-out-of-n: S 系统模型,并采用 Minkowski 距离和定义可生存性函数描述系统状态和可生存性。实验表明,MVL 条件下的 k-out-of-n: S 模型很好地描述了系统的状态和可生存性。

关键词 k-out-of-n: S 系统,可生存性,二值逻辑,多值逻辑

Research on MVL k-out-of-n: S System

ZHENG Ji-Ping^{1,2} QIN Xiao-Lin^{1,2} SUN Jin¹

(College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)¹

(Institute of Information Security, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)²

Abstract Components have multi-states in complex network environment, and binary logic (BL) is very limited to describe this situation. So, multi-valued logic (MVL) is adopted to analyze component state in this paper. Further, k-out-of-n: S system model is emphasized. System state and survivability are described by Minkowski distance and our defined survivable function. Experiments show that our k-out-of-n: S system using MVL can be capable to describe system state and survivability.

Keywords K-out-of-n: S system, Survivability, Binary logic, Multi-valued logic

1 引言

信息安全已从传统的以防御为中心的机制转到以入侵容忍为核心的新一代安全机制。1985 年, J. Fraga 等人提出入侵容忍概念^[1], 引起信息安全领域学者的广泛研究, 已有大量的研究成果。在诸多入侵容忍技术中, 冗余技术被广泛应用到具有入侵容忍特征的可生存系统中。1980 年, k-out-of-n 系统^[2]首次被提出以来, 引起了广大研究者的兴趣, 在系统可靠性方面引起广泛的研究, 近年来主要集中于多状态系统即多态系统^[6]的研究。

在分布环境下, 复杂系统往往面临诸多安全事件, 如受到攻击、系统内部故障等, 因而呈现多种状态, 如: 运行正常、运行基本正常、最低限度运行、失效等。通过相关的系统状态和可生存性的描述, 可以有效协助非正常运行系统进行重新配置, 进而使系统恢复到正常状态。因此, 需要引入相关机制描述系统的状态以及可生存性。本文在已有多态 k-out-of-n 系统^[6~14]基础上, 提出二值组件状态和多值组件状态下系统状态和可生存性模型, 重点研究了多状态组件(多态组件) k-out-of-n: S(Survivable)系统的可生存性^[3,4], 引入相对 Minkowski 距离和可生存性函数对多态系统的可生存性进行量化。实验表明, MVL 条件下的 k-out-of-n: S 系统模型可以很好地描述复杂状态和可生存性。

2 BL 条件下的 k-out-of-n: S 系统

传统的系统组件* 状态符合二值逻辑(BL, Binary Log-

ic), 即状态为 1, 组件运行正常; 状态为 0, 组件失效。组件在遇到系统故障或受到外来攻击时由 1 状态转化到 0 状态。

定义 1 BL 条件下离散 k-out-of-n: S 系统满足以下条件:

$x_1, x_2, \dots, x_n$ 分别表示组成系统的 n 个组件状态, 其中: $x_i \in [0, 1], i=1, 2, \dots, n$;

某一时刻系统组件状态矢量 $\vec{X} = (x_1, x_2, \dots, x_n)$;

k-out-of-n: S(Survivable)系统状态函数:

$$\varphi_B(\vec{X}) = \sum_{i=1}^n x_i \geq k.$$

定义 1 描述了二值逻辑情况下离散 k-out-of-n: S 系统基本性质, 系统边界状态是 $\varphi_B(\vec{X}) = k$ 。此时, 系统的可生存性为零。一旦发生组件状态 $x_i: 1 \rightarrow 0$ 的变化, 则系统变得不可用, 即失效。因此, BL 条件下离散 k-out-of-n: S 系统生存性由系统的冗余程度决定, 相关评价系统生存性标准即为组件的冗余度。

$$\begin{matrix} & \text{site}_1 & \text{site}_2 & \dots & \text{site}_n \\ \begin{matrix} k_1 \\ k_2 \\ \vdots \\ k_m \end{matrix} & \begin{bmatrix} d_{11} & d_{12} & \dots & d_{1n} \\ d_{21} & d_{22} & & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m1} & d_{m2} & \dots & d_{mn} \end{bmatrix} \end{matrix}$$

图 1 BL 情况下离散 k-out-of-n: S 系统模型表示的冗余密钥分布

图 1 描述了采用二值逻辑情况下离散 k-out-of-n: S 系统

*)国家自然科学基金(60673127);江苏省高技术研究计划项目(BG2004005);航空科学基金(02F52033)。郑吉平 博士研究生, 主要研究方向: 数据库安全、网络安全;秦小麟 教授, 博士生导师, 主要研究方向: 安全数据库、空间数据库、时空数据库、GIS 等;孙 瑾 博士研究生, 主要研究方向: 计算机视觉、图像处理与分析。

* 文中假定系统组件满足独立均匀分布(i. i. d., Independent and Indentically Distributed)属性。

模型来表示文[5]中冗余密钥的分配。其中 $site_i (i=1, \dots, n)$ 表示分配密钥的站点, $k_j (j=1, \dots, m)$ 表示冗余的密钥分片, d_{ij} (d_{ij} 取值为 0 或 1) 表示站点 i 是否存在密钥分片 k_j 的一个拷贝, 1 表示存在一个复本, 0 表示该站点不存在相关复本。图 1 直观地表述了文[5]的思想。

3 MVL 条件下的 k-out-of-n: S 系统

大型复杂网络和数据库系统组件在遭受攻击 (Attacks)、出现故障 (Failures) 或发生意外事故 (Accidents) 时往往具有不同状态, 例如: 运行正常、运行基本正常、最低限度运行、失效等。在存在非 0 非 1 状态下, 传统的二值逻辑描述组件状态时显得无能为力。采用多值逻辑 (MVL, Multi-Valued Logic) 可以很好地描述此类系统。多值逻辑具有如下基本性质^[7]:

$$x_i \vee x_j = \max\{x_i, x_j\} \quad (1)$$

$$x_i \wedge x_j = \min\{x_i, x_j\} \quad (2)$$

$$x_1 x_2 \dots x_k \vee x_1 x_2 \dots x_k x_{k+1} = x_1 x_2 \dots x_k \quad (3)$$

3.1 k-out-of-n: S 系统的 MVL 模型描述

定义 2 MVL 条件下离散 k-out-of-n: S 系统满足以下条件:

$x_1, x_2, \dots, x_n$ 分别表示组成系统的 n 个组件状态, 其中: $x_i \in \{0, \dots, M\}, i=1, 2, \dots, n, M$ 表示组件的最佳状态, 0 表示失效状态;

某时刻系统组件状态矢量 $\vec{X} = (x_1, x_2, \dots, x_n)$;

$x_{i_1}, x_{i_2}, \dots, x_{i_k}$ 分别表示系统中组件状态最好的 k 个组件, 即满足:

系统状态函数为

$$\phi_M(\vec{X}) = x_{i_1} x_{i_2} \dots x_{i_k} \quad (4)$$

其中, $\forall x_j, x_j \in \{x_1, x_2, \dots, x_n\} \& x_j \notin \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}$, 满足 $x_j \leq k$ 。

定义 2 给出了通常情况下 k-out-of-n: S 系统的 MVL 模型描述, 即系统中组件都离散可用, 系统状态的好坏取决于状态最佳的 k 个组件中最差组件的状态, 即满足水桶原理。

定义 3 MVL 条件下线性连续 k-out-of-n: S 系统, 在定义 2 的前提下, 当 $i_1, i_2, \dots, i_k$ 满足:

(1) $i_1 < i_2 < \dots < i_k$, 其中 $i_j = 1, \dots, n, j=1, \dots, k$;

(2) $\forall j (j < k), i_{j+1} = i_j + 1$

则上述系统为 MVL 条件下的线性 k-out-of-n: S 系统, 此类系统为最简单的一种关联 (组件彼此相邻) 系统。

定义 4 MVL 条件下环形连续 k-out-of-n: S 系统, 在定义 2 的前提下, 当 $i_1, i_2, \dots, i_k$ 满足:

(1) $i_1 < i_2 < \dots < i_k$, 其中 $i_j = 1, \dots, n, j=1, \dots, k$;

(2) if $\exists s, t, i_s = n, i_t = 1$ then

$\forall j (j \in [1, s]), i_{j+1} = i_j + 1$ or $\forall j (j \in [t, k]), i_{j+1} = i_j + 1$
else $\forall j (j < k), i_{j+1} = i_j + 1$

则上述系统为 MVL 条件下的环形 k-out-of-n: S 系统。

定义 2~4 表示了 MVL 条件下三种不同 k-out-of-n: S 系统模型: 离散、线性和环形。实际情况下, 根据组件的相互关系不同, 采用不同类型的 k-out-of-n: S 系统模型。

3.2 k-out-of-n: S 系统的 MVL 生存性评价函数

复杂系统在遭受攻击、系统故障、失效等意外情况时, 需要相应的恢复机制进行恢复。相同系统状态的 k-out-of-n: S 系统由于组件状态的不同因而生存性存在差异: 生存能力强的系统较小调整相应组件状态就可以达到较好的系统状态;

而生存性较差的系统可能需要对组件做较大的调整才能达到相应的系统状态。因而通过定义生存性评价函数量化系统的可生存性。

定义 5 MVL 条件下 k-out-of-n: S 系统生存性评价函数:

$$Sur_M(\phi_M(\vec{X}), Dis_p(\vec{X}, \vec{J})) = \phi_M(\vec{X}) + Dis_p(\vec{X}, \vec{J}) \quad (5)$$

其中: $Dis_p(\vec{X}, \vec{J})$ 表示向量 $\vec{X}, \vec{J}$ 之间的相对 Minkowski 距离:

$$Dis_p(\vec{X}, \vec{J}) = \left[\frac{1}{n} \sum_{i=1}^n |x_i - j|^p \right]^{1/p} \quad (6)$$

当 $p=1$ 时为相对 Hamming 距离:

$$Dis_{Ham}(\vec{X}, \vec{J}) = \frac{1}{n} \sum_{i=1}^n |x_i - j| \quad (7)$$

当 $p=2$ 时为相对 Euclid 距离:

$$Dis_{Euc}(\vec{X}, \vec{J}) = \left[\frac{1}{n} \sum_{i=1}^n |x_i - j|^2 \right]^{1/2} \quad (8)$$

实际的复杂网络与数据库系统中, 每个组件所起的作用不尽相同。核心组件往往至关重要, 这些组件在面临攻击、失效或意外事故时需要依然能够完成任务, 即此类组件在系统的层次比较“高”, 非核心组件在面临入侵或受损时, 可以暂时挂起或停止, 这类组件在系统的层次比较低。根据组件的“高低”位置不同, 通过带权的相对 Minkowski 距离修改生存性评价函数。权重向量表示为: $\vec{W} = (w_1, w_2, \dots, w_n)$ 。

调整后的系统组件状态:

$$\vec{X} = [x_1 \ x_2 \ \dots \ x_n] \times \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = [w_1 x_1 \ w_2 x_2 \ \dots \ w_n x_n]$$

调整后的相对 Minkowski 距离表示为

$$Dis'_p(\vec{X}, \vec{J}) = \left[\frac{1}{n} \sum_{i=1}^n |w_i x_i - j|^p \right]^{1/p}$$

其中 $\vec{J} = (j, j, \dots, j)$ 。

多状态组件系统当一个组件状态变化, 例如遭受攻击或者系统故障情况下, 通过式 (4)、(5) 重新计算系统状态和相应的生存性。当面临多个组件发生变化时, 例如分布攻击或者同谋攻击时, 系统状态变更可以描述为: 攻击失效向量 $\vec{A} = (f_1, f_2, \dots, f_n)$, 其中 $f_i \in [0, 1], i=1, \dots, n$; 当 $f_i=0$ 时表示组件 i 没有受到攻击; 当 $f_i=1$ 时, 组件 i 被颠覆。相关系统组件状态修改为

$$\vec{X} = [x_1 \ x_2 \ \dots \ x_n] \times \begin{bmatrix} 1-f_1 \\ 1-f_2 \\ \vdots \\ 1-f_n \end{bmatrix} = [(1-f_1)x_1 \ (1-f_2)x_2 \ \dots \ (1-f_n)x_n]$$

受到攻击 $\vec{A}$ 时的相对 Minkowski 距离表示为

$$Dis_p(\vec{X}, \vec{J}) = \left[\frac{1}{n} \sum_{i=1}^n |(1-f_i)x_i - j|^p \right]^{1/p}$$

生存性评价函数更改为

$$Sur_M(\phi_M(\vec{X}), Dis_p(\vec{X}, \vec{J})) = \phi_M(\vec{X}) + Dis_p(\vec{X}, \vec{J}) = x_{i_1} x_{i_2} \dots x_{i_k} + \left[\frac{1}{n} \sum_{i=1}^n |(1-f_i)x_i - j|^p \right]^{1/p}$$

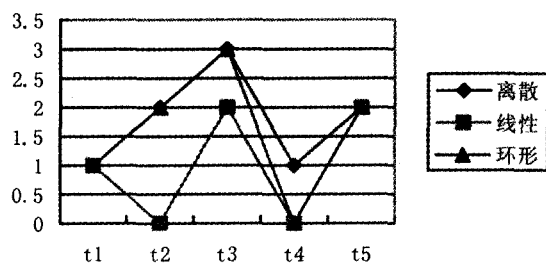
4 MVL 条件下 k-out-of-n: S 系统模型实验

实际情况下, k-out-of-n: S 系统状态受组件的权值、外来

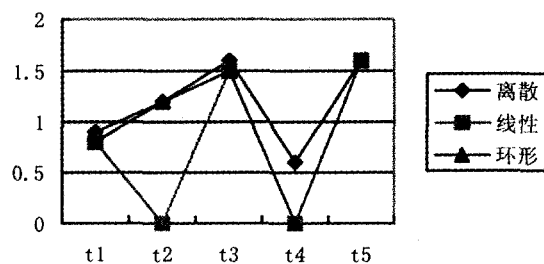
的攻击等因素影响,存在不同的状态,因而必须得到系统的实际状态,以便更好地分析和重新配置以恢复到正常状态。以 3-out-of-5: S 系统($k=3, n=5$)为例,其中 M 取 4, 即有 0, 1, 2, 3 种组件状态。给定权重向量 $\vec{W}=(0.6 \ 0.8 \ 0.8 \ 0.9 \ 0.5)$, 攻击失效向量 $\vec{A}=(0.2 \ 0.1 \ 0.3 \ 0 \ 1)$ 。随机给定不同时间的组件状态向量组成组件状态空间 M_S 、 MS_w 和 MS_a :

$$\begin{aligned} \vec{X}_{t_1} & \begin{bmatrix} 0 & 2 & 1 & 1 & 3 \\ 2 & 1 & 0 & 3 & 3 \\ 3 & 1 & 2 & 3 & 3 \\ 1 & 0 & 1 & 2 & 0 \\ 0 & 2 & 2 & 3 & 2 \end{bmatrix} & \vec{X}_{w_1} & \begin{bmatrix} 0 & 1.6 & 0.8 & 0.9 & 1.5 \\ 1.2 & 0.8 & 0 & 2.7 & 1.5 \\ 1.8 & 0.8 & 1.6 & 2.7 & 1.5 \\ 0.6 & 0 & 0.8 & 1.8 & 0 \\ 0 & 1.6 & 1.6 & 2.7 & 1 \end{bmatrix} \\ \vec{X}_{t_2} & \begin{bmatrix} 0 & 1.8 & 0.7 & 1 & 0 \\ 1.6 & 0.9 & 0 & 3 & 0 \\ 2.4 & 0.9 & 1.4 & 3 & 0 \\ 0.8 & 0 & 0.7 & 2 & 0 \\ 0 & 1.8 & 1.4 & 3 & 0 \end{bmatrix} & \vec{X}_{w_2} & \begin{bmatrix} 0 & 1.6 & 0.8 & 0.9 & 1.5 \\ 1.2 & 0.8 & 0 & 2.7 & 1.5 \\ 1.8 & 0.8 & 1.6 & 2.7 & 1.5 \\ 0.6 & 0 & 0.8 & 1.8 & 0 \\ 0 & 1.6 & 1.6 & 2.7 & 1 \end{bmatrix} \\ \vec{X}_{t_3} & \begin{bmatrix} 0 & 1.8 & 0.7 & 1 & 0 \\ 1.6 & 0.9 & 0 & 3 & 0 \\ 2.4 & 0.9 & 1.4 & 3 & 0 \\ 0.8 & 0 & 0.7 & 2 & 0 \\ 0 & 1.8 & 1.4 & 3 & 0 \end{bmatrix} & \vec{X}_{w_3} & \begin{bmatrix} 0 & 1.6 & 0.8 & 0.9 & 1.5 \\ 1.2 & 0.8 & 0 & 2.7 & 1.5 \\ 1.8 & 0.8 & 1.6 & 2.7 & 1.5 \\ 0.6 & 0 & 0.8 & 1.8 & 0 \\ 0 & 1.6 & 1.6 & 2.7 & 1 \end{bmatrix} \\ \vec{X}_{t_4} & \begin{bmatrix} 0 & 1.8 & 0.7 & 1 & 0 \\ 1.6 & 0.9 & 0 & 3 & 0 \\ 2.4 & 0.9 & 1.4 & 3 & 0 \\ 0.8 & 0 & 0.7 & 2 & 0 \\ 0 & 1.8 & 1.4 & 3 & 0 \end{bmatrix} & \vec{X}_{w_4} & \begin{bmatrix} 0 & 1.6 & 0.8 & 0.9 & 1.5 \\ 1.2 & 0.8 & 0 & 2.7 & 1.5 \\ 1.8 & 0.8 & 1.6 & 2.7 & 1.5 \\ 0.6 & 0 & 0.8 & 1.8 & 0 \\ 0 & 1.6 & 1.6 & 2.7 & 1 \end{bmatrix} \\ \vec{X}_{t_5} & \begin{bmatrix} 0 & 1.8 & 0.7 & 1 & 0 \\ 1.6 & 0.9 & 0 & 3 & 0 \\ 2.4 & 0.9 & 1.4 & 3 & 0 \\ 0.8 & 0 & 0.7 & 2 & 0 \\ 0 & 1.8 & 1.4 & 3 & 0 \end{bmatrix} & \vec{X}_{w_5} & \begin{bmatrix} 0 & 1.6 & 0.8 & 0.9 & 1.5 \\ 1.2 & 0.8 & 0 & 2.7 & 1.5 \\ 1.8 & 0.8 & 1.6 & 2.7 & 1.5 \\ 0.6 & 0 & 0.8 & 1.8 & 0 \\ 0 & 1.6 & 1.6 & 2.7 & 1 \end{bmatrix} \end{aligned}$$

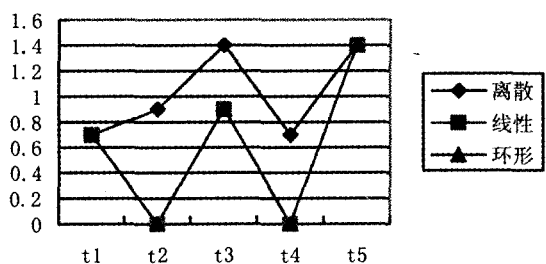
图 2 通常情况、带权重和受攻击状态下的组件状态空间



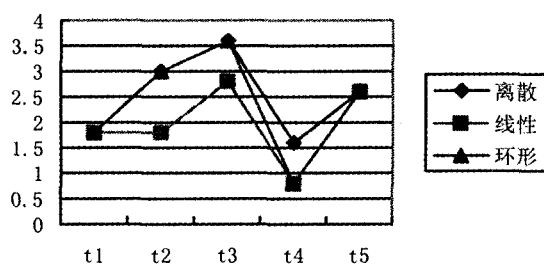
(a) 不同类型 3/5: S 系统函数对比



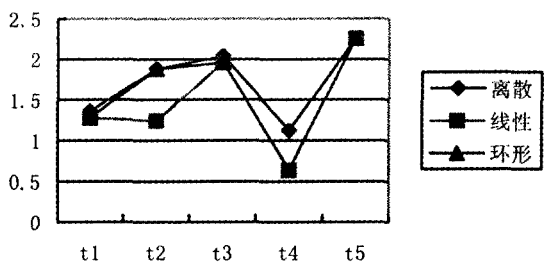
(b) 带权重不同类型 3/5: S 系统函数对比



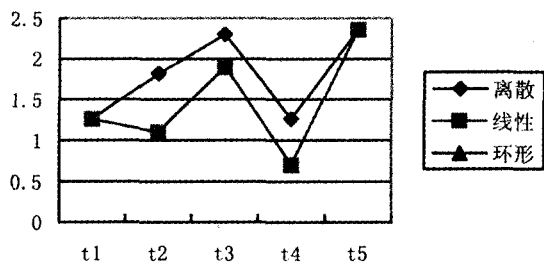
(c) 攻击情况下不同类型 3/5: S 系统函数对比



(d) 不同类型 3/5: S 系统生存性对比



(e) 带权重不同类型 3/5: S 系统生存性对比



(f) 受攻击时不同类型 3/5: S 系统生存性对比

图 a~c 中纵坐标表示系统状态函数值, 图 d~f 中纵坐标表示系统可生存性评价函数值

图 3 不同条件下的各种类型 3-out-of-5: S 系统状态和可生存性对比(其中横坐标表示时间)

态恢复问题。实验表明, MVL 条件下的 k -out-of- n : S 模型很好地描述了系统的状态和可生存性。未来的研究工作主要解决组件状态连续变化条件下系统状态变化的情形^[15], 同时考虑组件不满足 i. i. d. 条件下的系统状态和可生存性。

参考文献

- 1 Fraga J, Powell D. A Fault and Intrusion-tolerant File System [A]. In: Proc. of the 3rd Intl Conf. on Computer Security [C],

- 1985, 203~218
- 2 Kontoleon J M. Reliability determination of a r-successive-out-of-n; F system [J]. IEEE Trans Reliability, 1980, 29(R-29): 290~294
- 3 Stavridou V, Dutertre B, Riemenschneider R A, et al. Intrusion Tolerant Software Architectures [A]. In: Proc. of the DARPA Information survivability Conference and Exposition [C], 2001
- 4 Knight J C, Sullivan K J, Elder M C, et al. Survivability Architectures; Issues and Approaches [A]. In: Proceedings of the 2000 DARPA Information Survivability Conference and Exposition [C], Jan. 2000. 25~27
- 5 Wu T, Malkin M, Boneh D. Building intrusion tolerant applications [A]. In: Proceedings of the 8th USENIX Security Symposium [C]. USA, USENIX Association, August 1999. 79~91
- 6 Huang J, Zuo M J, Fang Z. Multi-state consecutive k-out-of-n systems [J]. IIE Transactions on Quality and Reliability Engineering, 2003, 35: 527~534
- 7 Zaitseva E N, Levashenko V G, Matiasko K, et al. Dynamic Reliability Indices for k-out-of-n Multi-State System [A]. In: International Symposium on Multiple-Valued Logic [C], May 2005. 264~269
- 8 Zuo M, Fang Z, Huang J, et al. Performance Evaluation of Decreasing Multi-State Consecutive-k-out-of-n; G Systems [J]. International Journal of Reliability, Quality and Safety Engineering, 2003, 10(3): 345~358
- 9 Lin M S. An $O(k^2 * \log(n))$ Algorithm for Computing the Reliability of Consecutive - k-out -of-n; F Systems [J]. IEEE Transactions on Reliability, 2004, 53(1): 3~6
- 10 Huang J, Zuo M J, Wu Y. Generalized multi-state k-out-of-n; G systems [J]. IEEE Transactions on Reliability, 2000, 49(1): 105~111
- 11 Amari S V, Pham H, Dill G. Optimal Design of k-out-of-n; G Subsystems Subjected to Imperfect Fault-Coverage [J]. IEEE Trans on Reliability, 2004, 53(4): 567~575
- 12 Boland P J, Samaniego F. Stochastic Ordering Among Consecutive k-out-of-n systems [J]. IEEE Transactions on Reliability, 2004, 53(1): 7~10
- 13 Cott D W, Liu J. System Reliability Optimization with k-out-of-n Subsystems [A]. International Journal of Reliability, Quality and Safety Engineering [C], 2000, 7(2): 129~142
- 14 Zaitseva E, Kovalik S, Levashenko V, et al. Reliability Analysis of the k-out-of-n Multi-state System [A]. In: First International Workshop on Model, Design and Validation [C], Nov. 2004. 51~57
- 15 Guima T A, Tapia M A. Differential Calculus for Fault Detection in Multi-valued Logic Networks [A]. ISMVL-87 - 17th International Symposium on Multiple-valued Logic [C], 1987. 99~108

全国高等师范学校计算机教育研究会

征文通知

为了进一步活跃高等师范学校计算机学术研究的氛围,全国高等师范学校计算机教育研究会决定,2008年征集学术论文及教育研究方面的论文选录,在《计算机科学》杂志正式出版的论文集中发表,欢迎大家积极投稿。现将征文的有关事宜通知如下:

一、征文内容

1. 计算机科学技术与应用学术论文
2. 计算机科学教育研究论文

二、征文要求

1. 论文必须未公开发表过,字数不超过5000字(含图表)。
2. 论文应包括题目(含英文题目)、作者姓名、作者单位、城市、邮编、英文摘要、英文关键词、正文(格式见附件)、参考文献格式为:

序号 作者·书名·出版社所在地: 出版社名, 出版年代

序号 作者·论文名·出处, 年代·卷号(期号): 起讫页码

3. 论文一式两份,一律以单面、隔行、A4纸激光打印。

4. 务必附上中文题目、中文摘要、第一作者姓名、单位、通信地址、邮编、电话和Email地址。

三、征文截止日期 2008年2月28日前(以邮戳为准)。

四、征文投递地址 400715 重庆市北碚区西南大学计算机与信息科学学院资料室

五、联系电话 (023) 68252389

全国高等师范学校计算机教育研究会