第36卷 第19期 计 算 机 工 程 2010年10月
Vol.36 No.19 Computer Engineering October 2010
·博士论文· 文章编号：1000—3428(2010)19—0014—04 文献标识码：A 中图分类号：TP391

基于混合法的监控系统可靠性分析

于 敏[a]，何正友[b]，钱清泉[b]
(西南交通大学 a. 信息科学与技术学院；b. 电气工程学院，成都 610031)

摘 要：针对复杂监控系统规模庞大及关键设备为双机冗余结构的特点，提出以动态故障树(DFT)为基础并结合蒙特卡罗方法对监控系统进行可靠性分析的混合方法。利用 DFT 建立系统可靠性模型，通过蒙特卡罗仿真算法对模型进行仿真计算，得到系统的可靠性指标。通过对地铁车站级监控系统的可靠性分析，证明了该模型的可行性和算法的有效性。

关键词：监控系统；动态故障树；蒙特卡罗方法；可靠性分析

Reliability Analysis of Monitor System Based on Hybrid Method

YU Min[a], HE Zheng-you[b], QIAN Qing-quan[b]
(a. School of Information Science & Technology; b. School of Electric Engineering, Southwest Jiaotong University, Chengdu 610031, China)

【Abstract】 For dealing with the large scale characteristic of complex monitor system as well as redundant structures of critical components, a hybrid method of reliability analysis for monitor system is presented on basis of dynamic fault tree and in combination with Monte Carlo simulation algorithm. Dynamic Fault Tree(DFT) is used to establish the reliability model of monitor systems. Reliability indices can be obtained by Monte Carlo method, which is used to solve the reliability model. A special reliability analysis case of the subway station-level monitor system is proposed, it demonstrates the feasibility of the model and the effectiveness of the algorithm.

【Key words】 monitor system; Dynamic Fault Tree(DFT); Monte Carlo method; reliability analysis

1 概述

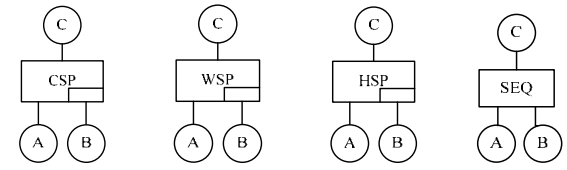
监控系统是实现监视控制与数据采集功能的系统，完成远方现场运行参数与开关状态的采集和监视、远方开关的操作、远方参数的调节等任务，并为采集到的数据提供共享的途径[1-2]。监控系统作为一种保证复杂系统正常工作与提高其运行可靠性的重要手段已经被广泛应用[3]。

对系统进行可靠性分析时，经常采用静态(传统)故障树模型及其相应的处理方法。但在工程中，监控系统的关键设备诸如服务器、网络设备等多采用双机冗余结构，而传统故障树方法用于描述冗余部件之间的顺序失效以及动态冗余管理机制时存在局限。因此，可引入动态故障树(Dynamic Fault Tree, DFT)对其进行可靠性分析。DFT 是在传统故障树基础上引入新的逻辑门来表征动态系统故障行为，常利用 Markov 状态转移过程进行计算，但它的计算量将随着系统规模的增大呈指数增长[4]，且 Markov 过程仅适用于失效与维修时间变量服从指数分布的情况。文献[5]提出利用基于梯形公式的顶事件概率计算法，但仍然存在组合爆炸的问题，并不适用于大型监控系统分析。而蒙特卡罗方法作为一种以概率统计理论为基础的数值计算方法，其计算量不受系统规模的制约[6]。结合 DFT 具有建模物理概念清楚的特点，本文提出利用混合法对监控系统可靠性进行分析。

2 监控系统可靠性模型

2.1 动态逻辑门

DFT 指至少包含一个专用动态逻辑门的故障树，具有顺序相关性、容错性以及冗余等特性[3]，本文对监控系统可靠性分析可引入如图 1 所示的 4 个动态逻辑门。图 1(a)~图 1(c)为双机储备门，用于描述双机冗余子系统的状态与其主、备用设备状态之间的关系。其中，输入事件 A、B 分别用于描述主、备用设备的状态，输出事件 C 则用于描述双机冗余子系统的状态。若主设备的失效率为λ，备用设备的失效率一般为 $\alpha\lambda$，$0 \le \alpha \le 1$。当冷储备时备用设备故障率为 0，则 $\alpha = 0$；温储备时备用设备故障率小于主设备故障率，则 $0 < \alpha < 1$；热储备时主、备用设备的故障率相同，即有 $\alpha = 1$。图 1(d)为顺序与门，当且仅当事件按从 A 到 B 的顺序发生时，输出事件 C 才会发生。



(a)双机冷备门 (b)双机温备门 (c)双机热备门 (d)顺序与门

图 1 动态逻辑门

2.2 DFT 预处理

当使用混合法对监控系统可靠性进行分析时，根据系统的失效原因建立 DFT，DFT 的顶事件为系统的故障事件，底事件为设备的故障事件。但蒙特卡罗方法是依据静态故障树的结构函数作为仿真的逻辑关系，因此，仿真之前需对 DFT 进行预处理，将 DFT 转换成静态故障树的方法如下：

基金项目：国家自然科学基金资助项目(50878188)
作者简介：于 敏(1982－)，女，博士研究生，主研方向：大型监控系统可靠性分析；何正友，教授、博士生导师；钱清泉，教授、中国工程院院士
收稿日期：2010-04-18 **E-mail：**yugnm@163.com

(1)由于监控系统中双机冗余子系统中的主设备及备用设备与系统其他设备并不直接相互作用，因此在转换的过程中可将 DFT 中的双机储备门、输出事件以及 2 个底事件看成一个整体，并由双机储备门的输出事件作为静态故障树的底事件。

(2)对于顺序与门而言，将顺序条件事件看作一个新的独立的输入事件，并与原顺序与门的输入事件一起作为变换后与门的输入，则顺序与门可变换成与门。

经过上述预处理的 DFT 可看作静态故障树，其中，静态故障树的顶事件仍为系统的故障事件，底事件则为部件(为便于描述，将顺序条件与非双机冗余设备都称作部件)或双机冗余子系统的故障事件。

2.3 模型描述

对由 n 个设备组成的监控系统进行可靠性分析时，根据设备的失效原因建立的 DFT 中将有 n 个底事件。若 DFT 中存在 m 个顺序与门与 k 个双机储备门，当将该 DFT 转换成静态故障树时，m 个顺序与门将生成 m 个顺序条件事件，则相应的静态故障树中底事件为 k 个双机冗余子系统与 $n-2k+m$ 个部件的故障事件。

根据静态故障树得到系统的结构函数 $\phi(x)$，当引入时间参变量后结构函数用 $\phi[x(t)]$ 表示，$x(t)=[b_1(t),b_2(t),\cdots,b_i(t),\cdots,b_{n-k+m}(t)]$ 为系统状态变量，其中，$b_i(t)(i=\overline{1,n-k+m})$ 表示静态故障树中第 i 个底事件的状态变量，取：

$$b_i(t)=\begin{cases}1 & \text{在}t\text{时刻第}i\text{个底事件发生}\\ 0 & \text{在}t\text{时刻第}i\text{个底事件未发生}\end{cases}$$

用 $\phi(t)$ 表示顶事件在 t 时刻的状态变量，有：

$$\phi(t)=\begin{cases}1 & \text{在 }t\text{ 时刻顶事件发生}\\ 0 & \text{在 }t\text{ 时刻顶事件未发生}\end{cases}$$

为便于分析系统的可靠性特征，作以下假定：

(1)设备只有正常或故障 2 种状态，故障状态指设备处于维修或待修状态，正常状态则指设备处于工作或储备状态，设备之间的状态相互独立，即不考虑设备之间的相关性。

(2)当系统故障时，未故障的设备将停止工作，且在停止工作期间不会发生故障。

(3)设备故障后立即维修且修复为完全修复，并假定有足够的维修设备及人员，即设备不会处于待修状态。

(4)设第 j 个设备的工作时间与维修时间变量的分布函数分别为 $F_{0,j}(t)$、$F_{1,j}(t)(j=\overline{1,n})$，第 k 个顺序条件事件发生与不发生的时间变量的分布函数为 $G_{1,k}(t)$、$G_{0,k}(t)(k=\overline{1,m})$。

(5)设双机冗余子系统故障检测及成功切换的概率为 c，并设转换开关完全可靠且自动切换可在瞬间完成。

3 蒙特卡罗仿真算法实现

3.1 算法基本原理

本文利用 Matlab 软件编制蒙特卡罗仿真程序。首先设置系统仿真运行时间 T 及仿真次数 M，然后进行第 i 次仿真，即根据部件与双机冗余子系统的状态及系统的结构函数得到系统的状态数组，最后重复上述步骤，直到仿真运行 M 次，得到每次仿真时系统对应的状态数组 $S_i(i=\overline{1,M})$。

有了系统的状态数组便可以得到系统的可靠性指标，监控系统通常为可修复系统，常用可用度(A)、首次故障平均时间($mttff$)、平均工作时间(mut)、平均故障时间(mdt)、平均周期(mct)等指标对其可靠性进行表征，下面给出可靠性指标的计算表达式[7]。

(1)A 为 t 时刻系统处于工作状态的概率，其点估计值为：

$$\bar{A}_S(t)=1-\frac{1}{M}\sum_{j=1}^{M}\phi_j(t) \tag{1}$$

其中，$\frac{1}{M}\sum_{j=1}^{M}\phi_j(t)$ 等于 M 次仿真中系统在 T 时刻故障的次数。

(2)$mttff$ 指发生首次故障的平均时间，点估计值为：

$$\overline{mttff}=\frac{1}{M}\sum_{j=1}^{M}T_{1,j} \tag{2}$$

其中，$T_{1,j}$ 为系统首次故障的时间。

(3)mdt 为发生故障的平均时间，其点估计值为：

$$\overline{mdt}=\frac{1}{\sum_{j=1}^{M}K_{Fj}}\sum_{j=1}^{M}\sum_{i=1}^{K_{Tj}}T_{i+1,j}-T_{i,j} \tag{3}$$

其中，$T_{i,j}$ 满足 $\phi(T_{i,j})=1$；K_{Tj} 和 K_{Fj} 分别为第 j 次仿真中系统发生状态转移的次数和发生故障的次数。

(4)mut 为系统处于工作状态的平均时间，点估计值为：

$$\overline{mut}=\frac{1}{\sum_{j=1}^{M}K_{Wj}}\sum_{j=1}^{M}\sum_{i=1}^{K_{Tj}}T_{i+1,j}-T_{i,j} \tag{4}$$

其中，$T_{i,j}$ 满足 $\phi(T_{i,j})=0$；K_{Wj} 为第 j 次仿真中系统处于工作状态的次数。

(5)mct 为 mut 与 mct 之和，即：

$$\overline{mct}=\overline{mut}+\overline{mdt} \tag{5}$$

蒙特卡罗仿真算法流程如图 2 所示。

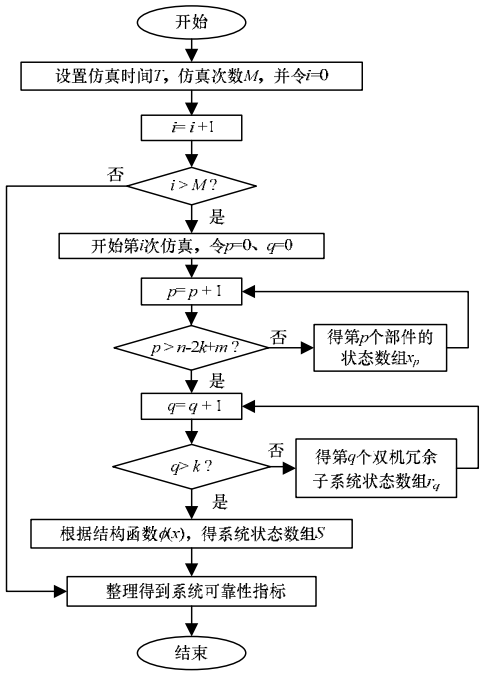


图 2 蒙特卡罗仿真算法流程

3.2 仿真过程分析

在第 i 次仿真时，首先对所有的部件、双机冗余子系统及整个系统的状态数组进行初始化，即分别利用 $zeros(1,T)$ 函数生成具有 T 个零元素的一维数组并记作 $x_p(p=\overline{1,n-2k+m})$、$r_q(q=\overline{1,k})$ 与 s_i；然后根据设备的工作时间与维修时间所服从的分布函数及顺序条件事件发生与不发生的时间变量的分布函数进行抽样，并通过分析确定部件、双机冗余子系统及整个系统在 t 时刻所处的状态，据此确定对应状态数组元素仿真之后的取值。

3.2.1　状态时间的抽样实现

本文利用直接抽样方法抽样设备或顺序条件事件处于各种状态的时间，对于随机变量 X 的分布函数 $F_X(x)$，记 $F_X^{-1}(x)$ 是 $F_x(x)$ 的逆函数，随机变量抽样的算法如下：(1)利用 Matlab 中的 *rand* 函数产生(0, 1)区间上服从均匀分布的随机数 η；(2)令 $x \leftarrow F_X^{-1}(\eta)$，即可以得到具有分布 F_X 的随机变量，再通过 *round* 函数对 x 进行取相邻整数运算，即可得到部件或顺序条件事件处于各种状态的时间。

3.2.2　部件状态数组赋值

对第 p 个部件状态数组进行赋值，首先初始化 $t=0$，若部件为设备时，则根据设备的工作时间的分布函数抽样工作时间 t_w，令 $t=t+t_w$；若 $t<T$，则继续抽样其维修时间 t_r，令 $t=t+t_r$；若仍有 $t<T$，则继续抽样 t_w、t_r 直到 $t \geq T$ 为止。若 $t(t=\overline{1,T})$ 时刻设备处于故障状态，则令 $x_p(t)=1$；否则，设备 t 时刻处于工作状态，$x_p(t)$ 为初值 0 不变。

若第 p 个部件为顺序条件时，其状态数组赋值的过程与部件为设备时相同，只不过设备的工作时间相当于顺序条件事件未发生的时间，设备的维修时间相当于顺序条件事件发生的时间。

3.2.3　双机冗余子系统状态数组赋值

本节描述第 q 个双机冗余子系统状态数组的赋值过程，子系统的工作原理为：主设备故障时由备用设备接替主设备继续工作，并对原主设备进行维修，待原主设备修复完毕时变成备用设备，当且仅当主设备与备用设备都故障时双机冗余子系统故障。

在仿真过程中，当双机冗余子系统备用设备故障或主设备与备用设备自动切换时，根据伪随机数 η 进行判断，若 $\eta \geq c$ 则故障检测或自动切换成功，否则故障检测或切换失败。根据工作时间分布函数抽样主设备与备用设备的工作时间并分析 t 时刻双机冗余子系统的状态，分为以下 4 种情况：

(1)当主设备与备用设备都为正常状态时，双机冗余子系统也为正常状态，则 $r_q(t)=0$。

(2)当主设备正常工作但备用设备故障时，若故障检测成功，则抽样备用单元维修时间；否则备用设备需直到主设备故障时才能抽样其维修时间，此时，双机冗余子系统仍为正常状态，令 $r_q(t)=0$。

(3)当主设备故障但备用设备可正常工作时，若自动切换失败，需要一个单位时间进行人工切换，则 t 时刻双机冗余子系统呈故障状态，令 $r_q(t)=1$；否则，主设备与备用设备自切换成功，双机冗余子系统仍为正常状态，则 $r_q(t)=0$；自动切换或手动切换完成后需继续抽样备用设备的维修时间。

(4)当主设备与备用设备同时处于故障状态时，双机冗余子系统处于故障状态，令 $r_q(t)=1$。

3.2.4　系统状态数组赋值

任意时刻 $t(t=\overline{1,T})$，部件的状态数组为 $x_p(t)(p=\overline{1,n-2k+m})$，双机冗余子系统的状态数组为 $r_q(t)(q=\overline{1,k})$，利用结构函数 $\phi(x)$ 对时刻 t 所对应的数组元素做布尔运算，若运算的结果为 0，则 $s_i(t)=0$；若运算的结果为 1，则令 $s_i(t)=1$，根据模型描述中的假定(2)，当系统故障时，未故障的设备将停止工作，且在停止工作期间不会发生故障。因此，在未故障的部件或双机冗余子系统对应的状态数组第 t 个元素至第 t+1 个元素之间插入一个值为 0 的元素，同时舍去数组最后一个元素，得到系统的状态数组 $s_i(t)$。

4　算例分析

为验证所建立的可靠性分析模型，本文以地铁车站级监控系统可靠性为例进行分析。地铁车站级监控系统对本站管辖范围内各监控对象的状态、性能等数据进行实时的收集，通过车站操作员工作站显示出来，并且可向分布在本站的被监控对象或系统发送模式控制、程序控制和点动控制等相关控制命令[3]，地铁车站级监控系统主要由实时服务器、操作员工作站、交换机、FEP 及以太网 5 部分构成。导致地铁车站级监控系统失效的主要原因如下：

(1)操作员不能通过工作站进行操作；

(2)车站实时服务器系统出现严重故障，无法工作；

(3)车站级局域网故障导致系统内各设备通信中断；

(4)FEP 失效，子系统上传来的信号不能有效的预处理。

根据设备的冗余模式及失效因素建立地铁车站级监控系统 DFT，如图 3 所示。

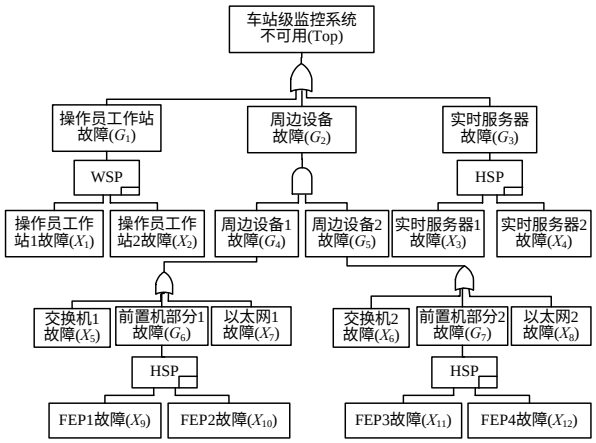


图 3　地铁车站级监控系统 DFT

对图 3 所示的 DFT 预处理，即利用双机储备门的输出事件表示 DFT 中的双机冗余子系统，得到 DFT 对应的静态故障树的结构函数为：

$$\phi(x)=G_1+G_2+G_3=G_1+G_4\cdot G_5+G_3= G_1+(X_5+G_6+X_7)\cdot(X_6+G_7+X_8)+G_3 \quad (6)$$

假设地铁车站级监控系统各设备的寿命及维修时间都服从指数分布，由设备的平均工作时间(*MTBF*)、平均维修时间(*MTTR*)得到设备的失效率与维修率如表 1 所示，其中，操作员工作站为双机温备方式，实时服务器与前置机为双机热备方式，冗余设备的故障检测及成功切换的概率 c 为 95%。

表 1　设备失效率及维修率

设备名称	*MTBF*/h	失效率	*MTTR*/h	维修率
操作员工作站(主)	300	0.003 3	10	0.100 0
操作员工作站(备)	500	0.002 0		
实时服务器	400	0.002 5	15	0.066 7
交换机	200	0.005 0	10	0.100 0
以太网	300	0.003 3	10	0.100 0
FEP	300	0.003 3	15	0.066 7

令仿真时间 M=2 000 h、仿真次数 M 为 10 000 次，对地铁车站级监控系统可靠性进行仿真得到的系统可用度曲线如图 4 所示。可以看出，地铁车站级监控系统可用度稳态值为 0.99。

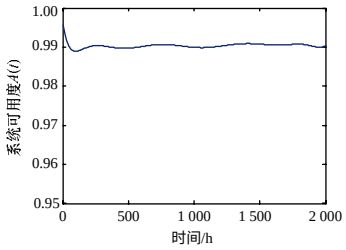


图 4　系统可用度曲线

地铁车站级监控系统系统其他可靠性指标点估计值如表 2 所示。

表 2　可靠性指标点估计值　　h

mttff	*mdt*	*mut*	*mct*
377	4	428	432

5　结束语

本文提出的基于混合法的监控系统可靠性分析方法综合了 DFT 的模型表达能力和蒙特卡罗仿真的方便性，避免了利用解析法计算可靠性指标时受系统规模限制的情况。该方法对设备的工作时间或维修时间服从威布尔分布、标准正态分布等其他非指数分布情况的适用性也很强，为复杂监控系统可靠性分析提供了有利工具。

参考文献

[1] 丁恩杰, 马方清. 监控系统与现场总线[M]. 江苏: 中国矿业大学出版社, 2003.

[2] 丁　飞, 张西良, 宋光明, 等. 面向设施环境的无线分布式监控系统[J]. 计算机工程, 2010, 36(3): 234-236.

[3] 吴　超. 地铁综合监控系统可靠性评估方法研究[D]. 成都: 西南交通大学, 2006.

[4] 陈光宇, 黄锡滋, 唐小我. 故障树模块化分析系统可靠性[J]. 电子科技大学学报, 2006, 35(6): 989-992.

[5] Amari S, Dill G, Howald E. A New Approach to Solve Dynamic Fault Trees[C]//Proc. of the International Conference on Reliability and Maintainability. Tampa, Florida, USA: [s. n.], 2003.

[6] 赵　耀, 韩泽耀, 付宇卓. 基于蒙特卡罗仿真的 LDPC 解码器功耗分析方法[J]. 计算机工程, 2009, 35(1): 216-218.

[7] 肖　刚, 李天柁. 系统可靠性分析中的蒙特卡罗方法[M]. 北京: 科学出版社, 2003.

编辑　顾姣健

（上接第 10 页）

5　结束语

本文采用(μ+λ)演化策略算法求解作业车间调度问题，并提出了一种基于工件操作次序的二维编码方法，对重组算子和变异算子进行了设计，通过典型算例的计算证明，演化策略算法能够有效地求解作业车间调度问题。

参考文献

[1] 玄光男, 程润伟. 遗传算法与工程优化[M]. 北京: 清华大学出版社, 2004.

[2] Brucker P. Scheduling Algorithm[M]. 5th ed. Berlin, Germany: Springer-Verlag, 2007.

[3] 黄　明, 宫　鹏, 梁　旭. 启发式 Hopfield 神经网络在车间调度中的应用[J]. 大连铁道学院学报, 2004, 25(1): 44-47.

[4] 童　刚, 李光泉, 刘宝坤. 一种用于 Job-shop 调度问题的改进禁忌搜索算法[J]. 系统工程理论与实践, 2001, 21(9): 48-52.

[5] 王　涛, 付宜利. 一种改进的遗传算法在车间调度中的应用[J]. 计算机集成制造系统, 2002, 8(5): 392-420.

[6] 王　凌. 车间调度及其遗传算法[M]. 北京: 清华大学出版社, 2003.

[7] 赵　军, 许玉龙, 孙晓静. 一种车间调度死锁实时解决算法[J]. 计算机工程, 2010, 36(5): 185-187.

[8] 赵良辉. 作业车间调度问题的文化算法[J]. 计算机工程, 2009, 35(13): 196-198.

编辑　张　帆

（上接第 13 页）

(4)接收到 I2 数据包，取出实名证书并验证，然后再进一步解决参数的验证。

为了能在 R1 和 I2 包中传送 IPv6 实名证书，本文在 HIP 协议中定义了一个新的证书参数，格式如图 6 所示，其中，Type 值为 768；Length 为证书的长度。HIP 协议规定新参数长度必须是 8 Byte 的整数倍，可以根据需要补充字节。

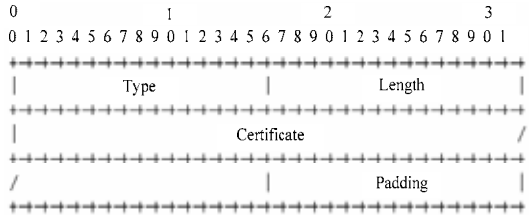


图 6　HIP IPv6 实名证书参数格式

5　结束语

本文提出的 IPv6 实名地址及实名地址 PKI 系统可以辅助 IPsec 完成端到端的身份认证和安全通信。该方法独立于上层应用，并能克服 IPsec 在标识符转换过程中有可能被屏蔽的固有缺陷，可以向上层应用提供实名通信服务。下一步需要在 IPv6 实名地址的身份管理框架下，继续进行行为和内容可信方面的研究工作，建立一个比较完整的可信解决方案。

参考文献

[1] 林　闯, 彭学海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751-758.

[2] Aura T, Roe M, Mohammed A. Experiences with Host-to-host IPsec[C]//Proc. of the 13th International Workshop on Security Protocols. Cambridge, UK: [s. n.], 2005.

[3] Moskowitz R, Nikander P, Jokela P. Host Identity Protocol[S]. RFC 5201, 2008.

[4] 甄鸿鹄, 陈　越, 李　乐. 基于身份的一次性公钥分析与重构[J]. 计算机工程, 2010, 36(1): 187-188.

[5] Lynn C, Kent S, Seo K. X.509 Extensions for IP Addresses and AS Identifiers[S]. RFC 3779, 2004.

[6] 徐迎晓. Java 安全性编程实例[M]. 北京: 清华大学出版社, 2003.

编辑　顾姣健