CRL 增量-过量发布综合模型研究*)

谭 良[1,2] 佘 堃[1] 周明天[1]

(电子科技大学计算机科学与工程学院 电子科技大学-卫士通信息安全实验室 成都610054)[1]

(四川师范大学软件重点实验室 成都610066)[2]

摘 要 针对当前PKI应用规模的变化,提出了一种新模型:增量-过量发布综合模型。该模型采用将Delta-CRLs的Base CRL过量发布来实现。通过比较表明,该方式既可以减小信任方下载的CRL大小,改善了响应时间,减少时间碎片;又可以降低对Base CRL峰值请求率,从而降低对存储库的峰值带宽和平均负荷。文中同时指出,增量-过量发布综合模型优于传统模型和增量模型,但其发布性能依赖于PKI系统的证书有效期、证书吊销率、Delta CRL的颁发周期和时间跨度。Delta CRL的颁发周期越长,时间跨度越大,证书吊销率越高,证书有效期越短,过量发布Base CRL所带来的性能优化就越小。因此,增量-过量模型适合于在Delta CRL的颁发周期和时间跨度较短、证书吊销率不高、证书有效期较长的大型PKI系统中。

关键词 证书撤消列表(CRL),增量CRL,过量发布CRL,增量-过量发布,证书吊销率,时间跨度,证书有效期,PKI

Research on the Delta and Over-Issued CRL Synthesis Model

TAN Liang[1,2] SHE Kun[1] ZHOU Ming-Tian[1]

(School of Comp. Sci. & Engn., Univ. of Electronic Sci. & Tech. of China, Information Security United Lab of UESTC-Westone, Chengdu 610054)[1]

(College of Electronic Engineering, Sichuan Normal University, Chengdu 610066)[2]

Abstract According to the change of application scale of PKI system currently, an improved model: the Delta and over-issued CRL synthesis model is presented, it is realized by that Base CRL of Delta-CRLs is over-issued. Compared to other models, the improved model minimizes the size of CRL which can accelerate to response time and time piece, as well as the peak request rate for Base CRL, the peak bandwidth and average loads on CRL repositories. Simultaneously it is presented in this paper that the improved model is better than traditional model and Delta-CRLs, but the issuance performance of the improved model depends on the rate of certificate revocation, period of certificate validity, time span and issue periods on Delta CRL. Rate of certificate revo-cation is more higher, time span and issue periods on Delta CRL is more longer and period of certificate validity is more shorter, the performance improvement by over -issued Base CRL is more less. So the improved model is fit for the large-scale PKIs whose rate of certificate revo-cation is not high, period of certificate validity is more longer, time span and issue periods on Delta CRL is more shorter.

Keywords Certificate revocation list(CRL), Delta-CRLs, Over-issued CRL, Delta and over-issued CRL, Rate of certificate revocation, Time span, Period of certificate validity, PKI

1 引言

证书撤销是公开密钥基础设施(PKI)中的一个关键性操作,运行PKI的开销主要来自证书撤消管理[1],为此,许多证书撤消机制被提出。目前,关于证书撤消问题的解决方案主要有X.509证书系统的证书撤消列表[2,3](Certificate Revocation List,简称CRL)、Micali的证书撤消系统[4](Certificate Revocation System,简称CRS)、Kocher的证书撤消树[5](Certificate Revocation Tree,简称CRT)以及Naor- Nissim的2-3证书撤消树(2-3CRT)[6]和线索二叉排序Hash树[7](certificate revocation threaded binary sorted hash tree,简称CRTBSHT)解决方案,但CRL是X.509证书系统中关于证书吊销问题的现行标准解决方案,商用CA或PKI系统主要使用定期颁布CRL来分发证书状态信息。

现有方法主要侧重通过更改X.509证书结构来对CRL的时间与空间特性进行改进,而对存储性能的优化,尤其是如何有效降低存储库峰值负荷方面仍有一些未解决的问题。为此,许多学者在这方面做了有益的探索,建立了多个数学模型,主要包括:分段CRLs[8],Delta-CRLs[9]和过量发布CRLs[10]。分段CRLs的峰值请求率不受CRL分段数的影响,但平均请求率随着分段数的增加而增加;Delta-CRLs减少CRL的大小,减少了耗费的峰值带宽和平均带宽,却不能减少峰值请求率,并且发布性能与时间跨度有关,时间跨度越大,发布性能越优化,但时间碎片问题越突出;过量发布CRLs降低了峰值请求率,时间碎片和可扩展性问题也得到改善,但是不能降低平均带宽,且CRL的发布频率提高了。这

*)基金项目:国家863计划项目(863-104-03-01)。谭 良 博士研究生,主要研究方向为网络计算,信息安全。佘 堃 在职博士生,主要研究方向为网络计算,信息安全。周明天 博士生导师,主要研究方向为网络计算,信息安全,分布式计算,并行计算。

些模型对如何优化 CRL 的存储性能、降低存储库峰值负荷、提高发布性能具有指导作用，但均不完善。特别是随着 Internet 的发展，CA 拥有的端实体数目迅速增加，端实体对 CRL 的发布性能提出了更高的要求。因此，这些发布模型对大规模的 PKI 系统是不实用的。

本文针对当前 PKI 应用规模的变化，分析了 CRL 发布证书状态信息的传统模型和增量模型及其存在的缺点，提出了一种新模型：CRL 增量-过量发布综合模型，该模型采用 Delta-CRLs 的 Base CRL 过量发布的方式来实现。通过分析表明，该方式既可以减小信任方下载的 CRL 大小，改善了响应时间；又可以降低对 Base CRL 峰值请求率，从而降低对存储库的峰值带宽和平均负荷。文中对增量-过量模型的性能参数进行了详细的推导和分析，并指出增量-过量模型适用于 Delta CRL 的颁发周期和时间跨度较短、证书吊销率不高、证书有效期较长的大型 PKI 系统。

2 PKI 应用规模的变化

X.509最初是在20世纪80年代中期开始设计的，那时的 Internet 没有像现在这样爆炸性地发展，它们被设计为在离线环境中运行。在这种情况下，计算机只是偶尔地连接起来，使用 CRL 的方式非常简单。

随着 Internet 的发展，PKI 的应用规模逐渐增加，CA 拥有的端实体数目迅速增加，CRL 可能变得很大，分发 CRL 将占用太多的网络资源，信任方得到它可能会困难，因为它们访问 CA 的带宽是有限的。并且由于 CRL 是由 CA 签过名的，在使用之前必须检验它的签名，检验一个庞大的 CRL 签名，所花的时间将会很长。再则，随着 CRL 的增大，对信任方和应用程序提出了更大的存储要求。同时，随着 CA 拥有的端实体数目迅速增加，CRL 库不能很好处理进来的所有访问，特别是请求率达到高峰时，部分请求失去了合理的响应时间。

最后，随着端实体的增加，部分端实体对 CRL 所含撤消信息的及时性提出更高要求，因为 CRL 是定期发布的，而撤消请求的到达是随机的，从接收撤消请求到下一个 CRL 发布之间的时延所带来的状态不一致性会严重影响由 PKI 框架提供的 X.509证书服务的质量。为解决这个问题，一方面，可以对 CRL 的分发机制进行改进，减小 CRL 发布的时间碎片；另一方面，可以采用 OCSP(Online Certificate Statues Protocol)。本文主要讨论前一种情况。

因此，大规模的 PKI 对 CRL 分发机制提出了更高的要求，就是尽可能减小信任方所需下载的 CRL 并应试图可以降低 CRL 峰值请求率、峰值带宽和平均负荷，减小时间碎片。

3 CRL 发布的传统模型和增量模型

为便于分析，假设信任实体的证书验证服从指数时间间隔的概率密度[11]，即不同信任实体验证行为的时间选择是相互独立的，信任实体除非执行一个验证，否则不会从存储库中请求证书吊销信息；并且将已下载的 CRL 缓存起来直到过期。

3.1 CRL 传统模型

传统的 CRL 发布模型认为：新 CRL 发布后，信任实体对存储库 CRL 请求满足指数分布规律。其概率密度函数为：

$$ve^{-vt}dt \tag{1}$$

其中，v 是确认率(单位时间信任实体企图确认证书的平均数量)。因为每个信任实体会在时刻0后执行第一次确认企图时下载 CRL，(1)式也就是任一给定信任实体在时间间隔$[t,t+dt]$内向 CRL 存储库发送请求的概率。(1)式乘以信任实体的总数 N，然后再除以 dt，即可得出在时刻 t 对 CRL 存储库的请求率：

$$R(t)_{trad}=Nve^{-vt} \tag{2}$$

假设 CRL 的有效期为 T_{trad}，则平均请求率为：

$$\overline{R(t)}_{trad}=\frac{1}{T_{trad}}\int_0^{T_{trad}}Nve^{-vt}dt=\frac{N}{T_{trad}}(1-e^{-vT_{trad}}) \tag{3}$$

假设每个 CRL 首部的大小为 S_H，CRL 中每项的大小为 S_E。假设系统中平均每天有 r 个证书被吊销，证书有效期平均为 L_C 天，每个证书从被吊销到该证书过期的平均时间为 $L_C/3$ 天。基于上述假设，一个完全 CRL 的平均大小为：

$$S_C=S_H+S_ErL_C/3$$

峰值带宽为：

$$B_{trad}=S_C\times R(0)=Nv(S_H+S_ErL_C/3) \tag{4}$$

平均负荷为：

$$\overline{B}_{trad}=S_C\times\overline{R(t)}_{trad}=\frac{N}{T_{trad}}(1-e^{-vT})(S_H+S_ErL_c/3) \tag{5}$$

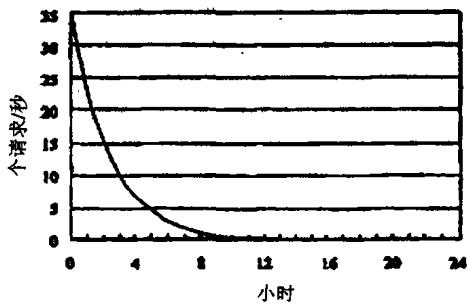


图1 传统模型的请求率

如果做如下假设：(1)CRL 的有效期是24小时；(2)CRL 在时刻0发布；(3)共存在300000个信任实体，即 $N=300000$；(4)每个信任实体平均每天确认10个证书，即 $v=10$；(5)系统中平均每天吊销1000个证书；(6)证书的平均有效期为365天。CRL 中每项大小为9个字节，那么 CRL 存储库的请求率如图1所示。

从图1可以看出，对于传统证书状态信息发布模型，每个信任实体所缓存的 CRL 会在同一时刻过期。CRL 过期后，新的 CRL 立即发布，每个信任实体为了执行确认必须从存储库获得新的 CRL，结果将导致在 CRL 发布后会有相当高的请求率，然后请求率以指数函数下降。如果 CRL 的有效期相当长，那么会有一段时间存储库基本上没有请求。图1所示最初请求为34.72个/秒，12小时后下降到了0.24个/秒，到24小时，请求率仅为1.6×10^{-3}个/秒，平均请求率为3.47个/秒。峰值带宽36.26M 字节/秒，平均负荷为3.62MB 字节/秒。

3.2 增量 CRL 模型

Delta-CRLs 机制是在系统中采用两种证书撤销列表：Base CRL 和 Delta CRL。Base CRL 在其被发布时，包含当时所有的证书撤销信息。在 Base CRL 有效期内，系统可能还会撤销一些证书，这些证书的序列号就被记录在 Delta CRL 中，并被及时地发布出去。通常，Delta CRL 表项明显地小于 Base CRL，它的发布频率可以更高。在同一个 Base CRL 有效期内，可以及时地发布多个 Delta CRL。最新的 Base CRL 和最新的 Delta CRL 包含了所有已撤销但仍未过期的证书信息。使用 Delta CRL，Base CRL 的有效期就可以更长。

为便于讨论，我们将 Delta CRL 的时间跨度 T_Δ 定义为：Delta CRL 中所参考的 Base CRL 与该 Delta CRL 在颁发时

间间隔上的最小值。Delta CRL 的时间跨度 T_Δ 的值是变化的，取决于颁发 Delta CRL 的方式。设 T_0 为 Base CRL 的颁发周期，T_1 为 Delta CRL 的颁发周期。一般情况下，T_0 为 T_1 的整数倍，即 $T_0=kT_1$。因此，Delta CRL 与所参考的 Base CRL 在颁发时间上的间隔，即时间跨度 T_Δ 可表示为：nT_1，其中，$0\leqslant n\leqslant k-1$。

在使用 Delta CRL 情况下，信任实体一次验证将导致至少一次对 Delta CRL 的请求，以及可能的第二次对 Base CRL 的请求。因此，对 Delta CRL 的请求率将与传统方式下对完全 CRL 的请求率相同。

对于 Base CRL 的获取，或者从储存库中下载，或者在本地由一个 Delta CRL 及一个早先的 Base CRL 构造而成，信任实体可使用 Delta CRL 更新其本地缓存而不必获取新的 Base CRL。设系统中最新的 Delta CRL 中参考的 Base CRL 在时刻0颁发，则在时刻 t，一个信任实体从储存库中请求一个 Base CRL 当且仅当此时是它从该 Base CRL 颁发以来第一次执行验证。因此，对 Base CRL 的请求率将与传统方式下对 CRL 的请求率相同，从而有：

$$R(t)_{Base}=Nve^{-vt} \tag{6}$$

可以看到，式(6)与式(2)在形式上是完全一致的，但参数 t 的含义是不同的。式(6)中，参数 t 表示从系统中最近的 Delta CRL 中所参考的 Base CRL 颁发以来到目前为止的时间，其值域为 $[T_\Delta,\cdots,T_\Delta+(k-1)T_1]$，其中 T_Δ 为 Delta CRL 的时间跨度，T_1 为 Delta CRL 的颁发周期。因此，Base CRL 的峰值请求率为：

$$Nve^{-vT_\Delta} \tag{7}$$

式(7)是关于时间跨度 T_Δ 的函数且呈指数递减。对 Base CRL 的平均请求率为：

$$\overline{R(t)}_{Base}=\frac{1}{(T_0-T_\Delta)}\int_{T_\Delta}^{T_0}Nve^{-vt}dt=\frac{N}{(T_0-T_\Delta)}(e^{-vT_\Delta}-e^{-vT_0}) \tag{8}$$

由于 Delta CRL 中所包含的证书状态变化信息在时间上的跨度是变化的，为便于计算 Delta CRL 的大小，取其最大值，有：

$$S_\Delta=S_H+S_{Er}[T_\Delta+(k-1)T_1] \tag{9}$$

因此，对于 Delta CRLs 峰值带宽 $B_{Delta\text{-}CRLs}$，有：

$$B_{Delta-CRLs}=S_CNve^{-vT}+S_\Delta Nv \tag{10}$$

平均带宽 $\overline{B}$，有：

$$\overline{B}_{Delta\text{-}CRLs}=S_C\times\frac{N}{(T_0-T_\Delta)}(e^{-vT_\Delta}-e^{-vT_0})+S_\Delta\times\frac{N}{T_\Delta}(1-e^{-vT_\Delta}) \tag{11}$$

从(10)式可以看到，峰值带宽 $B_{Delta\text{-}CRLs}$ 是关于时间跨度 T_Δ 的函数，其值由两部分组成，一部分是关于 Base CRL 的带宽，呈指数递减；另一部分是关于 Delta CRL 的带宽，呈线性递增。对(10)式求解 $dB_{Delta\text{-}CRLs}/dT_\Delta=0$，有：

$$T_{max}=(\frac{1}{v})\ln[v(S_H+1/3S_{Er}L_c)/S_{Er}] \tag{12}$$

当 T_Δ 取 T_{max} 时，系统中的峰值带宽将达到最小。

假如 Base CRL 的颁发周期为24小时，Delta CRL 的颁发周期为15分钟，时间跨度等于 Delta CRL 的颁发周期15分钟，仍以3.1节所做的假设为例，则 Delta CRL 的峰值请求率为34.72个/秒，Base CRL 的峰值请求率为31.29个/秒，峰值带宽为：31.29×(51+3×1000×365)+34.72×(51+94)字节/秒，峰值带宽从36.26MB 字节/秒，降低到32.68MB 字节/秒，下降约9.87%。Base CRL 平均请求率3.16个/秒，平均带宽为3.16×(51+3×1000×365)+3.47×(51+94)=3.30MB 字节/秒，降低约8.82%。考虑增加时间跨度，取 n=8，此时，Delta CRL 的时间跨度等于2小时，则 Delta CRL 的峰值请求率不变，Base CRL 的峰值请求率为15.09个/秒，峰值带宽为：15.09×(51+3×1000×365)+34.72×(51+750)=15.79MB /秒，下降约56.47%；Base CRL 平均请求率1.50个/秒，平均带宽为1.50×(51+9×1000×365)+3.47×(51+844)=1.57MB/秒，降低约56.65%。

通过(12)式计算出的 T_{max} 为17小时，此时 Base CRL 的峰值请求率为 2.85×10^{-2} 个/秒的峰值带宽达到最小值0.24MB 字节/秒，降低约99.33%，平均请求率 9.30×10^{-3} 个/秒，平均带宽达到最小值 3.13×10^{-2}MB 字节/秒，降低约99.13%。

从上面的分析可以看出，存储库采用 Delta-CRLs 发布方式，峰值带宽和平均负荷有所降低，但降低的程度与时间跨度有关，在区间 $[0,T_{max}]$，峰值带宽和平均负荷随着 T_Δ 的增大而减小；在区间 $[T_{max},\infty]$，峰值带宽和平均负荷随着 T_Δ 的增大而增大；当 $T_\Delta=T_{max}$ 时，峰值带宽和平均负荷达到最小值。因此，Delta-CRLs 发布方式要获得较好的性能，则 T_Δ 在 $[0,T_{max}]$ 内应尽量取得更大，但 T_Δ 越大，Delta-CRLs 发布方式的时间碎片问题越突出，并且 Delta-CRLs 并没有降低总的峰值请求率，因此，Delta-CRLs 方式不适合大规模 PKI 的要求。

4 增量-过量发布综合模型

传统模型和增量模型都不适合大规模 PKI 的 CRL 发布需求。为了提高 CRL 的发布性能，减小信任方所需下载的 CRL 并降低 CRL 峰值请求率、峰值带宽和平均负荷，减小时间碎片，可以采用令 Delta-CRLs 的时间跨度 T_Δ 在区间 $[0,T_{max}]$ 尽量取一个合适的值，满足时间碎片的要求，然后将 Delta-CRLs 的 Base CRL 在 T_0 内过量发布来实现，即将减小时间碎片而引起的 CRL 峰值请求率、峰值带宽和平均负荷的增加通过过量发布 Base CRL 来适当弥补。下面建立增量-过量发布 CRL 综合模型。

4.1 增量-过量发布综合模型的建模过程

把 Base CRL 发布所隔时间定义为一个时间间隔，前文已经提到一个信任实体仅仅在给定时间间隔内需要执行一次确认而且它的缓存中不存在未过期的 Base CRL 时才会向存储库发送一个请求。如果 O 代表给定时间间隔内有效的 Base CRL 的数量，P_{val} 代表信任实体在给定的时间间隔内对 Base CRL 执行确认的概率，则信任实体在时间间隔 q 请求 Base CRL 的概率为 P_{val} 乘以其在前 $q-1$ 个时间间隔内没有执行确认的概率，即

$$p_{i,q}=p_{val}[1-\sum_{j=q-o+1}^{q-1}p_{i,j}] \tag{13}$$

当系统处于稳定状态时，信任实体在连续的发布周期内对 Base CRL 执行确认的概率将相同，即

$$p_{i,q}=p_{i,q-1}=\cdots=P_{i,1} \tag{14}$$

所以在稳定状态下：

$$p_i=p_{val}[1-(O-1)p_i] \tag{15}$$

解得：

$$p_i=p_{val}/[(O-1)p_{val}+1] \tag{16}$$

如果时间间隔从0时刻开始，那么信任实体在时间 t 到 $t+dt$ 内向 CRL 存储库发送请求 Base CRL 的概率等于信任实体

在时间段 t 到 $t+dt$ 内对 Base CRL 执行它的第一次确认请求的概率乘以信任实体在缓存中没有以前时间间隔有效的 Base CRL 的概率，信任实体在$[t,t+dt]$内向 Base CRL 发送请求的概率由(1)式确定；信任实体在缓存中没有有效 Base CRL 的概率可以通过信任实体在时间间隔内请求 Base CRL 的概率除以信任实体在时间间隔内对 Base CRL 执行确认的概率计算出来(即式(16)除以 P_{val})。这样，信任实体在$[t,t+dt]$内请求 Base CRL 的概率为：

$$\frac{ve^{-vt}dt}{(O-1)P_{val}+1} \tag{17}$$

由于确认呈指数概率分布，信任实体在给定发布周期对 Base CRL 不执行确认的概率为 $e^{-vT_0/O}$，这里 T_0为 CRL 的有效期，T_0/O 即为一个时间间隔，所以：

$$P_{val}=1-e^{-vT_0/O} \tag{18}$$

带入(17)式，得：

$$\frac{ve^{-vt}dt}{(O-1)(1-e^{-vT_0/O})+1} \tag{19}$$

(19)式子乘以信任实体总数 N 再除以 dt，得在时刻 t 对 Base CRL 的总请求率：

$$\frac{Nve^{-vt}}{(O-1)(1-e^{-vT_0/O})+1} \tag{20}$$

注意，对于增量-过量发布模型，时间 t 的值域应为：$[T_\Delta,\cdots,T_\Delta+(k-1)T_1]$，取时间的初始值为 T_Δ，对 Base CRL 的峰值请求率为：

$$R(0)=\frac{Nve^{-vT_\Delta}}{(O-1)(1-e^{-vT_0/O})+1} \tag{21}$$

当 CRL 不断发布时即$\lim O\to\infty$，有

$$\lim_{O\to\infty}\left[\frac{Nve^{-vT_\Delta}}{(O-1)(1-e^{-vT_0/O})+1}\right]=\frac{Nve^{-vT_\Delta}}{vT_0+1} \tag{22}$$

(22)式代表了增量-过量 CRL 发布综合模型在理论上对 Base CRL 可达到的最小峰值请求率，但实际中达到最小峰值请求率是不可能的。

Base CRL 的有效期为 T_0，则增量-过量 CRL 发布综合模型对 Base CRL 的平均请求率为：

$$\overline{R(t)}=\frac{1}{T_0-T_\Delta}\int_{T_\Delta}^{T_0}\frac{Nve^{-vt}}{(O-1)(1-e^{-vT_0/O})+1}dt=\frac{N(e^{-vT_\Delta}-e^{-vT_0})}{(T_0-T_\Delta)[(O-1)(1-e^{-vT_0/O})+1]} \tag{23}$$

当 CRL 不断发布时即$\lim O\to\infty$，有：

$$\lim_{O\to\infty}\frac{N(e^{-vT_\Delta}-e^{-vT_0})}{(T_0-T_\Delta)[(O-1)(1-e^{-vT_0/O})+1]}=\frac{N(e^{-vT_\Delta}-e^{-vT_0})}{(T_0-T_\Delta)(vT_0+1)} \tag{24}$$

(24)式代表了增量-过量 CRL 发布综合模型在理论上对 Base CRL 可达到的最小平均请求率，但实际中达到最小平均请求率是不可能的。

增量-过量 CRL 发布综合模型的峰值带宽为：

$$B_{Delta-Overissued-CRLs}=S_\Delta Nv+\frac{S_CNve^{-vT_\Delta}}{(O-1)(1-e^{vT_0/O})+1} \tag{25}$$

增量-过量 CRL 发布综合模型的峰值带宽的极限为：

$$(B_{Delta-Overissued-CRLs})_{\min}=S_\Delta Nv+\frac{S_CNve^{-vT_\Delta}}{vT_0+1} \tag{26}$$

平均带宽为：

$$\overline{B}_{Delta-Overissued-CRLs}=S_C\times\frac{N(e^{-vT_\Delta}-e^{-vT_0})}{(T_0-T_\Delta)[(O-1)(1-e^{-vT_0/O})+1]}+S_\Delta\times\frac{N}{T_\Delta}(1-e^{-vT_\Delta}) \tag{27}$$

平均带宽的极限为：

$$(\overline{B}_{Delta-Overissued-CRLs})_{\min}=S_C\times\frac{N(e^{-T_\Delta}-e^{-vT_0})}{(T_0-T_\Delta)(vT_0+1)}+S_C\times\frac{N}{T_\Delta}(1-e^{-vT_\Delta}) \tag{28}$$

假如 Base CRL 的颁发周期为24小时，Delta CRL 的颁发周期为15分钟，时间跨度为2小时，$O=8$，仍以第1部分所做的假设为例，则 Delta CRL 的峰值请求率为34.72个/秒，Base CRL 的峰值请求率为2.52个/秒，峰值带宽为：2.52×(51+3×1000×365)+34.72×(51+750)=2.66MB 字节/秒，峰值带宽从36.26MB 字节/秒，降低到2.66MB 字节/秒，下降约92.68%。Base CRL 平均请求率为0.25个/秒，平均带宽为0.25×(51+3×1000×365)+3.47×(51+844)=0.26MB 字节/秒，降低约92.70%。当 $O=16$时，Base CRL 的峰值请求率为1.89个/秒，峰值带宽为：1.89×(51+3×1000×365)+34.72×(51+750)=2.00MB /秒，峰值带宽下降约94.48%。Base CRL 平均请求率为0.19个/秒，平均带宽为0.19×((51+3×1000×365)+3.47×(51+844)=0.20MB/秒，降低约94.49%。

通过(22)、(24)式可计算出增量-过量模型性能参数的极小值，此时 Base CRL 的峰值请求率为1.37个/秒，峰值带宽达到最小值1.46MB/秒，降低约95.98%，平均请求率0.14个/秒，平均带宽达到最小值0.15MB/秒，降低约95.99%。

4.2 比较分析增量模型和增量-过量发布综合模型

从上面的分析可以看出，Delta-CRLs 发布方式要获得较好的性能，则 T_Δ在$[0,T_{max}]$内应尽量取得更大，但 T_Δ越大，Delta-CRLs 发布方式的时间碎片问题越突出，并且 Delta-CRLs 并没有降低峰值请求率。而增量-过量将减小时间碎片而引起的峰值带宽和平均负荷的增加通过过量发布 Base CRL 来适当弥补，不仅可以降低 Base CRL 的请求率，从而降低总的请求率；而且可以降低时间碎片。因此增量-过量模型在发布性能上优于传统模型和增量模型。

增量-过量模型主要是靠过量发布 Base CRL 的方式来降低峰值请求率和平均请求率，从而降低峰值带宽和平均带宽。从(25)式可以看出，CRL 发布耗费的总带宽由两部分组成，其中 $S_\Delta Nv$ 表示 Delta CRL 的峰值带宽，S_Δ由(9)式决定；$\frac{S_CNve^{-vT_\Delta}}{(O-1)(1-e^{vT_\Delta/O})+1}$是 Base CRL 的峰值带宽，$S_C=S_H+S_{ER}L_C/3$。当一个 PKI 系统采用增量-过量模型发布 CRL 时，如果该系统的证书吊销率大，Delta CRL 的时间跨度 T_Δ和颁发周期长，$S_\Delta Nv$ 增加得快；如果该系统的证书有效期小，$\frac{S_CNve^{-vT_\Delta}}{(O-1)(1-e^{vT_\Delta/O})+1}$就减小得快，则：

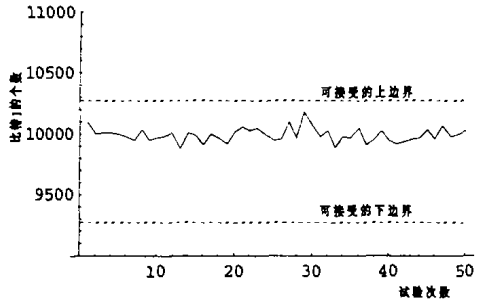
$$S_\Delta Nv>\frac{S_CNve^{-vT_\Delta}}{(O-1)(1-e^{vT_\Delta/O})+1}$$

所需要的时间越短，Base CRL 此时过量发布 Base CRL 降低的峰值带宽所占的比例较小，总的峰值带宽主要由 Delta CRL 的峰值带宽决定，过量发布 Base CRL 的意义不大，这使得对增量-过量模型的使用受到一定的限制。对平均带宽也有类似的结论。因此，增量-过量模型适合于在 Delta CRL 的颁发周期和时间跨度较短、证书吊销率不大、CRL 有效期较小的大型 PKI 系统中。

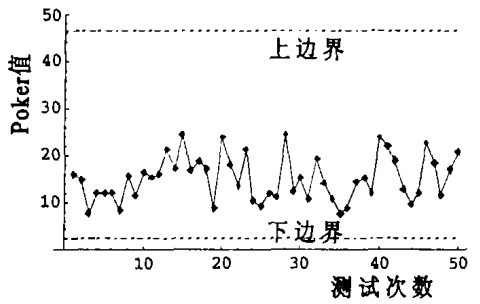
结论 本文分析了发布证书的传统模型，针对当前 PKI 应用规模的变化，提出了一种新的模型：增量-过量发布综合模型。通过比较可以看出，该方式既可以减小信任方下载的

(下转第139页)

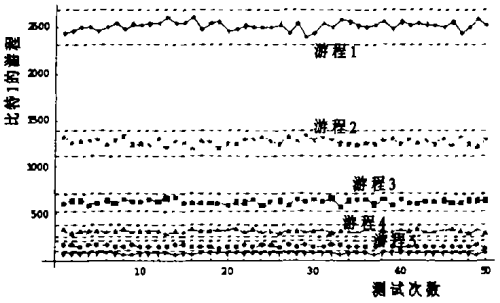
测试5项基本测试[2]。对产生的20000比特伪随机数序列进行测试，若任何一个测试没有通过，则认为没有通过 FIPS 的随机性测试。本文采用两种方法来生成检验的20000比特：a)元胞空间大小为50，运行400时步，生成长度为400的50个随机时间序列，把这50个随机序列连接起来，构成长度为20000比特的序列；b)元胞空间大小为50，运行8时步，然后把50个长度为8比特连接起来构成400比特，这个过程重复50次得到长度为20000比特的随机序列。按照这个测试标准要求，每种方法各进行了50次试验，部分试验结果如图1所示。



(a) 频率测试/单比特测试结果



(b) 扑克测试结果



(c) 游程测试结果结果

图1 GA-CA 随机数发生器生成伪随机数的统计检验结果

从测试结果可以看出，用遗传算法获得的扩展元胞自动机规则可以产生高质量的伪随机数，均全部通过。说明采用遗传算法来生成扩展元胞自动机的规则是可行的，同时也说明，生成的伪随机数满足美国联邦数据处理标准中加密模块的要求。

结论 元胞自动机固有的结构和演化规则简单，而其状态既不可预测又瞬息万变的特性，为随机现象模拟提供了得天独厚的条件。本研究利用这一基本特性，进行了元胞自动机的一维扩展，并结合遗传算法的优化搜索功能，构造出 GA-CA 模型——一维扩展元胞自动机的伪随机数发生器生成模型。试验结果表明，该发生器能生成随机性良好的伪随机数，经统计检验，完全通过美国联邦信息处理标准(FIPS140-2)，满足加密模块的要求。扩展元胞自动机可以快速地生成高质量的伪随机序列，特别适用于需要快速加密的场合。同时这种伪随机数发生器也可以方便地用硬件实现，可以用于 VLSI 内建自测试以及并行计算等多种领域。混合元胞自动机扩展了均匀元胞自动机的应用范围，拓展了元胞自动机的发展应用空间，为密码学等领域应用提供一种简单快速的伪随机数发生器。

一维扩展元胞自动机的演化状态，在一定程度上受到有限邻居的制约。如果构造出二维扩展元胞自动机模型，伪随机数的性质将会得以更大提高。

元胞自动机演化规则确定之后，初始状态则直接影响未来的演化状态，而"求优"实乃在限定空间的"最优化"。若把总体优化与局域优化兼用，例如人工神经网络、支持向量机等方法与遗传算法结合，可能构造出更优秀的随机数发生器。以上两点也正是我们进一步研究的内容。

参 考 文 献

1 Tomassini M, et al. Generating high-quality random numbers in parallel by cellular automata. Future Generation Computer Systems, 1999, 16(2-3): 291～305

2 Tomassini M, Perrenoud M. Cryptography with cellular automata. Applied Soft Computing Journal, 2001, 1(2): 151～160

3 Seredynski F, Bouvry P, Zomaya A Y. Secret Key Cryptography with Cellular Automata. In: Proc. of the Intl. Parallel and Distributed Processing Symposium (IPDPS'03), Nice, France, 2003

4 Chopard B, Droz M. 物理系统的元胞自动机模拟. 祝玉学，赵学龙译. 北京：清华大学出版社，2003

5 FIPS. FIPS140-2: Security requirements for Cryptographic Modules. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. 2001

(上接第136页)

CRL 大小，改善了响应时间，减少时间碎片；又可以降低对 Base CRL 峰值请求率，降低峰值带宽和平均负荷。增量-过量模型适合于在 Delta CRL 的颁发周期和时间跨度较短、证书吊销率不高、证书有效期较长的大型 PKI 系统中。

参 考 文 献

1 Adams C, Farrell S. RFC2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols [s]. RFC2510, Internet Engineer TaskForce, March 1999

2 Rivest R L. Can we eliminate certificate revocation lists. In: Rafael H, ed. Financial Cryptography. Anguilla, 1998. British West Indies: Springer, 1997. 178～183

3 Hously R, Ford W, Polk W, et al. Internet X.509 public key infrastructure certificate and CRL profile. IETFRFC2459, 1999. http://www.ietf.org/rfc/rfc2459.html

4 Micali S. Efficient certificate revocation. TechnicalMemory, MIT/LCS/TM-5426, 1996. http://www.lcs.mit.edu/pub-lications

5 Kocher P. On certificate revocation and validation. In: Hirschfeld, R., ed. Financial Cryptography-FC'98. LNCS1465, Berlin: Springer-Verlag, 1998. 171～177

6 Moni Naor, Kobbi Nissim. Certificate revocation and certificate update. IEEE Journal on Selected Areasin Communications, 2000, 18(1): 561～170

7 王尚平，张亚玲，王育民. 证书吊销的线索二叉排序 Hash 树解决方案. 软件学报，2001，12(9)：1343～1350

8 Arnes A, Just M, Knapskong S J, et al. Selecting revocation solutions for PKI. Paper Submitted to NORSEC2000, 2000

9 Cooper D A. A more efficient use of Delta-CRLs. In: Proc. of the 2000 IEEE Symposium on Security and Privacy, 2000. 190～202

10 David A C. A Model of Certificate Revoction [C]. In: Proc. 15th Annual, Computer Security Applications Conference, 1999. 256～264

11 David A C. A closer look at revocation and key compromise in public key infrastructures[ED/CD]. http://csrc.nist.gov/nissc/1998/proceedings/paperG2.pdf, 1998-10-11