一种基于 P2P 共享下载模式的证书撤销机制

李国敬[1,2]，温 涛[1]

(1.东北大学 信息科学与工程学院，辽宁 沈阳 110004；2.中共烟台市委党校，山东 烟台 264000)

摘 要：基于增量 CRL 证书撤销机制，提出了基于 P2P 共享下载模式的证书撤销机制。在 Delta-CRL 的发布周期内，CA 发布 Base-CRL 和 Delta-CRL，用户除初始化外，其他时刻只需下载 Delta-CRL 即可。当用户提出请求，通过洪泛机制查询相应节点和资源的信誉度记录，找到最优记录节点，建立 P2P 连接。然后，将下载的 CRL 模块在客户端重构以获得完整的 CRL。与其他 CRL 相比，该方法能够有效减少 CRL 的下载尺寸，真正降低通信载荷以及系统的峰值请求率，提供更为及时的证书撤销信息。

关键词：公钥基础设施；证书撤销列表；信誉度；P2P 模式

中图分类号：T309.7 **文献标识码**：A **文章编号**：1674-7720(2011)07-0050-03

Research on certificate revocation mechanism based on P2P shared download scheme

Li Guojing[1,2] Wen Tao[1]

(1.Information Science and Engineering College, Northeastern University, Shenyang 110004, China;
2.Party School of Yantai Commitee, CPC, Yantai 264000, China)

Abstract: Based on Delta-CRL, the paper proposes a revocation scheme based P2P shared download mechanism. During the issuing period of Delta-CRL, CA issues Base-CRL and Delta-CRL. Users at the clients only need to download Delta-CRL except for initialization. When a user requires for download through flooding, it inquires the related node's resource and node credit records. It finds out the right node and creates P2P connection. Thus total CRL will be obtained by reorganization in the clients. Comparing to other CRL schemes, the scheme can efficiently decrease the download size of CRL, lower the traffic load and release the average request frequency of the system. It will provide more timely certificate information.

Key words: PKI; CRL; credit; P2P scheme

公开密钥基础设施 PKI (Public Key Infrastructure)是以公开密钥密码技术为基础、提供安全服务的具有通用性的安全基础设施，在网络传输与交换过程中可以提供身份鉴别、完整性、不可否认性和机密性的信息安全服务。数字证书主要通过数字签名和加密功能来实现安全通信的功能。在确认交易之前，验证方必须检查证书的有效性，确保持证者身份真实、合法、有效，这样就可以降低网络环境下的交易风险，保证电子商务安全、公正。然而证书在发布后，其合法性会随着时间的推移以及突发的或某些特殊原因而变为无效，因此，在证书发行之后，认证中心(CA)将发布证书撤销列表 CRL(Certificate Revocation List)供用户查询验证证书的有效性。

传统的证书撤销机制有基本 CRL(Base-CRL)、分段 CRL[1]、重复发布 CRL[2]、增量 CRL(Delta-CRL)[3]、随机 CRL 证书撤销机制[4]等，这些证书撤销机制分别在如何提高 CRL 的传输与查询效率、减少通信载荷和计算代价、降低峰值请求率、提供及时性等方面对 CRL 证书撤销机制作了一定的改进，以适应不同的应用需求。本文以改进的增量 CRL 证书撤销机制[5](简称 ICRL)为基础，提出点对点(P2P)共享下载模式，为客户端提供 CRL 列表，以供用户在本地进行证书的验证。这种模式能够有效减少 CRL 的下载尺寸，真正降低通信载荷以及系统的峰值请求率，提供更为及时的证书撤销信息。

1 P2P 共享下载模式原理

1.1 基本原理

如果文件大小在 150 MB 以上，可以采用P2P 技术上

的文件共享软件下载模式。这种下载模式与传统文件共享下载模式的区别是:共享文件不是在集中的服务器上等待用户端来下载,而是分散在所有参与者的硬盘上。所有参与者组成一个虚拟网络,每个用户端都可以从这个虚拟网络里的任何一个人的计算机里下载文件,同时每个人也可以把自己的文件共享给任何人。

图1为ftp、http等分享下载流程,P2P共享下载模式的分享流程如图2所示。

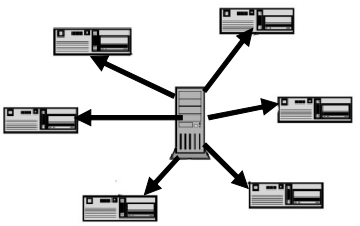

图1 ftp.http等分享下载流程

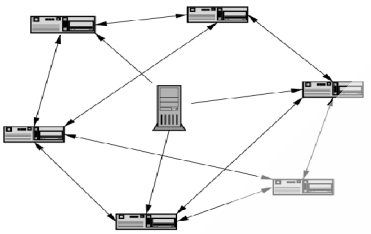

图2 P2P共享下载模式的分享流程

这种P2P共享下载模式的典型代表为BT(BitTorrent)、ED和EM。以BT为例介绍其原理。BT首先在CA服务器端把一个文件分成了Z个部分,甲在服务器随机下载了第N个部分,乙在服务器随机下载了第M个部分,这样甲的BT就会根据情况到乙的电脑上去下载乙已经下载好的M部分,乙的BT就会根据情况到甲的电脑上下载甲已经下载好的N部分,这样不但减轻了服务器端的负荷,也加快了用户方(甲、乙)的下载速度,提高了效率,同时减少了地域之间的限制。例如,丙要连到服务器去下载可能速度较慢(只有几K),但是要是到甲和乙的电脑上去下载就快得多了。客户端在下载的同时,也在上传文件,下载的人越多,下载的速度也越快。所以在峰值请求时,服务器的负担得以减轻,并且客户端下载的速度也越快,这就是BT的优越性。

BT使用了分布式计算的概念,让每一个对等节点参与到通信协作中来,充分利用每一个节点的上载能力,使得传输一个文件的实际带宽数十倍、百倍、千倍地扩大。

1.2 P2P下载模型

应用P2P方式组织下载CRL列表时,所有参与下载的可信CA、不可信的目录服务器、验证方以及最终用户都加入到P2P网络中,所有参与者都提供上传与下载服务。

CA参照ICRL证书撤销机制[5],在发布CRL时,一方面发布最新和完整的CRL列表(Total-CRL),同时又发布Base-CRL和Delta-CRL供用户下载。CA将Total-CRL和Base-CRL根据需要分成了Z个部分。更新周期到达时,目录服务器、验证方等用户可以到CA随机地下载CA的各个部分。随着时间的推移,加入P2P网络的用户就能以一定的策略选择网络中的终端进行CRL的下载。

1.3 CRL的重组

与ICRL证书撤销机制相同,P2P模式下载得到的CRL需要在本地进行重组,以剔除过期的证书,得到最新的、完整的CRL证书撤销列表,以供验证方使用。

重组过程可以参照ICRL证书撤销机制,与之不同的是,由于P2P模式下,验证方下载的CRL有可能是从不可信的第三方(客户端或参与验证的第三方),而不是从可信的CA那里获得到的CRL,不可信的客户端有可能进行重放攻击,伪造虚假的CRL列表,从而妨碍CRL列表的正常下载与重组,所以验证方就要在本地通过比对CA签名验证下载CRL的有效性。一旦下载的CRL不可靠,则必须重新选择下载服务器,下载可靠的CRL列表。在最坏情况下,客户端必须重新从CA下载CRL列表信息。

2 客户端信誉度评价

2.1 风险与安全性分析

P2P系统自由开放的特性也为其应用带来了一定的风险隐患,如:不可信的客户端进行重放攻击,伪造虚假的CRL列表妨碍CRL列表的正常下载,由于网络性能差造成客户端下载的不稳定,客户端自由地进出P2P系统和中止服务以及拒绝服务攻击、客户端的在线时间等。

用户一方面可以根据X.509的定义,通过检查CRL列表中的This update和Next update字段来判断所下载证书是否为最新,以抵御重放攻击。另一方面可以通过CA提供的签名来验证CRL是否为伪造。对于假冒的非CRL证书信息则比较容易判断。

为使客户端在P2P系统顺利、及时地下载到可靠的CRL列表,就必须选择信誉好的客户端。为此,就必须对参与提供下载服务的客户端进行信誉评价,以便让验证方选择信誉度高的客户端,这样才能最大限度地保证验证方能够下载到最及时、完整、可靠的CRL列表。

2.2 信誉度模型

系统中主要涉及资源信誉度RC (Resource Credit)和节点信誉度NC(Node Credit)。资源信誉度是指节点提供的CRL列表是否可靠,同时体现节点提供CRL分块的下载量;而节点信誉度是指某个节点是否能够及时、正确无误地提供CRL分块的下载,同时也体现了节点的在线时间以及稳定性等因子。

(1)资源信誉度$RC(x)$

一个资源信誉度的值由历史信誉度值和新的评价

值共同合成。

$$RC(x)=\alpha\cdot RC_{old}(x)+\beta\cdot RC_{new}(x) \quad (1)$$

$$RC_{new}(x)=x\frac{\sum D_r}{D}-\delta\left(1-\frac{\sum D_r}{D}\right) \quad (2)$$

$0\leqslant\alpha,\beta\leqslant1,0\leqslant x,\delta\leqslant1$

其中，α、β 分别表示各自对信誉度的影响率，$RC_{new}(x)$ 表示上一评价周期过后产生的信誉度的计算。D_r 为从节点中下载 CRL 资源 r 的总量，D 为节点 x 所提供 CRL 资源的总量，x、δ 分别为影响因子。

信誉度是一个随时间变化的量，同时也与下载是否能顺利进行相关，所以本系统采用时间驱动和事件驱动相结合的评价机制。设评价周期为 T，如果在 T 内，CRL 资源没有在系统中被下载，则其资源信誉度更新为：

$$RC(x)=(1-\varepsilon)RC_{old}(x),0\leqslant\varepsilon\leqslant1 \quad (3)$$

(2)节点信誉度 $NC(x)$

$$NC(x)=\alpha\cdot\frac{\sum C_x}{C}-\beta\cdot\frac{\sum D_x}{D}+\gamma\cdot\frac{\sum T_x}{T}-\delta\cdot F_{x-rate} \quad (4)$$

$0\leqslant\alpha、\beta、\gamma、\delta\leqslant1$

其中，x 为节点标示，$\sum C_x$ 为从该节点下载的可信 CRL 模块的总量（字节数），C 为该节点提供的所有 CRL 资源总量，$\sum D_x$ 为从该节点下载的不可信 CRL 资源总量，D 为该节点提供的所有 CRL 资源总量（$D=C$），$\sum T_x$ 为节点的在线时间，T 为节点进入系统以来的时间，F_{x-rate} 为违约率。

与资源信誉度类似，如果节点在某一个评估周期内没有提供资源、资源没有被下载或没有在线时间，则节点信誉度的更新方法为：

$$NC(x)=(1-\varepsilon)NC_{old}(x),0\leqslant\varepsilon\leqslant1 \quad (5)$$

2.3 信誉度系数取值

在提出的信誉度模型中，各个系统的取值没有直接依据，这和系统追求的目标以及经验有关。在资源信誉度模型中，式(1)和式(2)中系数取值体现两种因子的权重，可以令 $\alpha+\beta=1$、$x+\delta=1$，也可以统一按对应因子的重要程度对 α、β、x、δ 分别取值。例如，设 $\varepsilon>x$，则表示系统更关心下载资源违约的情况。在节点信誉度模型中，应根据因子的重要程度对 α、β、γ、δ 分别取值。如为了体现不可信 CRL 资源对信誉度影响更大，β 值应比较大。违约是严重影响信誉度的事件，因此，所对应的系统不宜太小，特别在节点信誉度的评估中，其他系统可以做简单的平均取值。

2.4 信誉度初值

信誉度是对一个节点的历史给予评价，而对于刚加入系统的节点，由于其没有提供上传及下载服务，其信誉度的初值不能为 0，如果为 0，则被选中的机会很少。因此，可设其信誉度的初值为一个平均值，以保证其有机会被选中。

2.5 信誉度更新

信誉度更新可以采用时间驱动和事件驱动更新两种方法。时间驱动更新可以定期或不定期地根据现有基础数据进行信誉度评估；事件驱动更新则是发生的某一动作或事件导致某一信誉度评价的基础数据发生变化。事件驱动更新能及时准确地反映信誉度的变化。在节点没有下载服务时，其信誉度应该降低。在这种情况下应该采用时间驱动更新服务，以随时更新节点信誉度。所以本系统采用事件与时间驱动相结合的更新方式。

2.6 信誉度管理与下载服务器的选择

在信誉度的管理中，可以采用有统一中心节点的管理模式。但是由于中心节点存在瓶颈问题，一旦中心节点瘫痪，整个系统也将崩溃。另外，由于 P2P 模式的自组织特性，也不便于使用中心节点模式。因此，在本系统中，每一个加入网络的用户自己维护一张信誉度表格。当用户需要在系统中下载资源时，提出请求通过洪泛机制，然后查询相应节点和资源的信誉度记录，找到最优记录的节点，然后节点之间可以直接建立连接。

假定某个节点 A 已在网络中，当一个新节点 B 加入系统中时，节点 A 中的表格中给该新节点 B 设定初值，而 B 节点则在表格中将系统中的其他节点设定初值。随着下载服务的进行，不断更新每一个节点的信誉度值。总是给 CA 设定一个中间值，以保证 CA 不会被最先选到，但又能在其他服务器失效时，提供下载服务。对于系统中已有节点也可仿照此法设定初值。

如果一个节点在较长时间内(如 6 个月)没有登录或者没有提供下载服务，则删除节点记录。

用户在选择下载服务器时，总是综合考虑选择信誉度大的节点进行资源下载，如果失败，则顺序选择信誉度次大的节点。

系统也可以将资源信誉度和节点信誉度进行合并，按照权重进行计算、优选。将资源信誉度和节点信誉度分开，可以根据用户所关心方面的不同，进行合理选择下载服务器。

3 性能分析

当一个提供 CRL 分块下载服务的节点中的 CRL 分块不可靠时(是伪造的或者其来源本身就不可靠)，那么随着时间的推移，其资源信誉度将越来越低。反之，当一个节点提供的资源可信时，其资源信誉度也越高。

当一个节点本身不可靠、网络质量差、节点不稳定或不提供下载服务，那么它的节点信誉度值也将逐渐降低。而提供良好下载服务的节点将会得到较高的信誉度。

传承 ICRL 的优点，本文提供的 CRL 证书撤销机制，可以最大限度地降低通信载荷，节约带宽。同时，由于系统将下载服务分散到各个参与者服务器中，因此大大降低了 CA 的平均及峰值请求率，减轻了 CA 服务器的负担。

由于 P2P 方式是一种自组织的分享下载方式，验证方下载 CRL 要依赖于其他下载用户同时在线提供上传服务来提高下载速度，这是不可靠的服务，因此其性能有一定的不稳定性。

综上所述，P2P 共享下载模式，能为客户端提供 CRL 列表，以供用户在本地进行证书的验证。这种模式能够有效减少 CRL 的下载尺寸，真正降低通信载荷以及系统的峰值请求率，提供更为及时的证书撤销信息。但是，P2P 方式下载是一种自组织的分享下载方式，当同时下载人数数量太少时，它的优势根本不能体现，验证方下载 CRL 要依赖于其他下载用户同时在线提供上传服务来提高下载速度，这是不可靠的服务。P2P 下载模式可以通过对 CRL 列表文件进行哈希生成摘要以抵御安全性攻击，但是共享系统中也有可能产生假冒 CA 发布 CRL 或拒绝服务攻击，因此存在一定缺陷。

参考文献

[1] AARNES A, JUST M, KNAPSKOG S J, et al. Selecting revocation solutions for PKI [C]. Proceedings of the Fifth Nordic Workshop on Secure IT Systems (NORDSEC 2000). Reykjavik, Iceland, 2000:360-376.

[2] COPPER D A. A model of certificate revocation [C]. Proceedings of 15th Annual Computer Security Application Conference, Phoenix, 1999: 256-264.

[3] COOPER D A. A more efficient use of delta-CRLs [C]. Proceedings of the 2000 IEEE Symposium on Security and Privacy, Berkeley, 2000: 190-202.

[4] 李国敬.随机 CRL 证书撤销机制研究[J].沈阳理工大学学报,2006(4):13-15.

[5] 李国敬，温涛.基于增量的 CRL 证书撤销机制研究[J].广西师范大学学报,2008(4):51-53.

(收稿日期:2010-11-09)

作者简介：

李国敬，男，1971 年生，副教授，博士研究生，主要研究方向：信息安全、知识组织。

温涛，男，1963 年生，博士生导师，主要研究方向：信息安全、知识组织。