分布式按需提供密码服务调用方案

王 曦[1] 赵洚伶[1] 周 波[1] 杜 薇[1]
WANG Xi ZHAO Cenling ZHOU Bo DU Wei

摘 要 随着云计算和大数据时代的到来，在去中心、大规模、高度动态的环境下，数据传输的安全与身份权限的合法性认证越来越受到关注，由此引入了各种类型业务应用对不同种类密码服务的需求。基于此种需求，对分布式网络环境下的多业务差异化密码服务调度方法进行研究。首先，提出一种基于熵权法的差异化密码服务评价方法；然后，利用 Gossip 协议，同步分布式节点间的负载信息；接着，结合前馈神经网络的负载预测，提出一种多业务差异化密码服务调度方案；最后，通过对比测试与分析，结果表明方案在保证密码服务高效调度的同时具有较强的扩展性与上限。

关键词 大数据；分布式；密码服务；神经网络；按需调度

doi：10.3969/j.issn.1672-9528.2024.06.041

0 引言

随着云计算与大数据技术的兴起，基于云计算和大数据平台的各种应用系统也应运而生。目前，面向智能电网、智慧水务、医疗诊断、高端制造等行业的云计算大数据平台应用较为广泛。随着企业业务的扩展，平台产生的数据量也成倍增长。在庞大且多样化的数据中，可能包含大量的机密信息。这些都是高附加值的数据，如果泄露可能会导致企业竞争力下降。因此，在云计算与大数据时代，数据安全的重要性不言而喻，而密码服务是保障数据安全的核心基础。

在复杂的云计算环境下，应用系统往往具有业务需求差异化较大、高并发和高随机性的特点。这也对密码服务的保障能力提出了更高的要求。因此，在保证高并发访问的同时，具备密码服务资源的动态按需调度能力，最大化释放底层算力，成为目前亟须解决的问题。

传统的密码服务调度策略要么无法满足大数据并发访问的需求[1]，要么不具备高效可靠的差异化密码服务调用能力[2]。针对以上问题，本文提出一种调度方案，既可满足业务数据集中访问，又可根据不同业务需求动态调度密码服务资源，优化了密码设备的服务供给能力，满足了不同应用系统的差异化需求，整体提升了大数据环境下的密码服务性能。本文的主要贡献如下。

（1）提出了一种基于前馈神经网络的密码服务负载预测模型。该模型通过任务参数作为输入，可以高效预测节点负载能力。同时结合基于熵权法的差异化密码服务评价模型与分布式负载信息同步模型，提出适用差异化密码服务器需求的分布式调度策略。该策略可以适应大并发访问和差异化服务需求。

（2）按照本文提出的分布式按需提供密码服务调用方案，实现了原型系统，并开展对比测试。测试结果表明，本文方案相比于其他两种方案在保证密码服务高效调度的同时具有较强的扩展性与较高的上限。

1 相关工作

近年来，资源调度算法一直是学术界的热点，学者们从各个角度展开研究，陆续取得了一些突破性成果。

Aroca 等人[3]、Duan 等人[4] 和 Maio 等人[5] 分别以降低数据中心能耗为目的，基于 CPU 为主要能耗源的场景，提出了虚拟机调度模型，在一定程度上克服了应用局限性的缺点，但在以密码资源需求为主导的密码服务集群环境中，能耗并不是系统负载均衡优化的第一目标。

Grandl 等人[6] 提出了 Altruistic 调度方法，将集群资源优先分配给时间较长的任务，但此方法无法对动态变化的任务需求实时调整调度策略。

杨婷等人[7] 提出了一种自适应权值最小负载的 LVS 集群负载均衡算法，该算法对加权最小连接算法做出一些改进，可在一定程度上提升负载效率，但可能出现超出节点最大负载导致任务请求丢失的情况。

You Liang 等人[8] 提出一种基于任务链的微服务负载均衡算法 TCLBM，通过减少物理机之间的数据传输来降低服务响应时间。李鑫等人[9] 提出了基于分布式遗传算法的负载均衡算法，该算法均衡效果优于传统算法。Li 等人[10] 也提出了一种基于虚拟化技术的密码资源管理框架，给出了一种

1. 中国电子科技集团公司第三十研究所 四川成都 610041

加密服务虚拟机的动态迁移方法，可以实现密码服务虚拟机的调度和迁移。但三者均未考虑动态变化的密码服务资源和差异化的密码服务需求。

寇文龙等人[11]针对差异化密码服务资源需求，提出了一种按需调度方案。但该方案无法解决中心节点的负载瓶颈问题。

目前的资源调度算法大多都未站在整个集群密码算力资源的角度进行考虑，而密码服务集群的特性决定负载均衡主要考量的是底层算力资源，同时还需根据密码服务集群和密码服务需求变化动态调整调度策略。

2 密码业务调度策略

本节主要从密码服务评价方法、负载信息传播模型和负载信息预测模型出发，提出一个密码业务调度策略。

2.1 基于熵权法的差异化密码服务评价方法

密码服务集群中各节点的各项资源状态存在复杂性和不确定性，服务能力存在差异性，同时用户方实时的调用需求也存在较大的随机性。基于资源负载情况等先验信息，使用香农信息熵的原理，对各类型密码资源负载信息进行权重统计处理，形成差异化密码服务集群的服务状态评价系数。

假设密码服务集群由数台配置不相同的服务器密码机组成，包括 n 台服务器，表示为集合 $R=\{r_1, r_2, \cdots, r_n\}$，集群包含 m 项密码服务，表示为集合 $S=\{s_1, s_2, \cdots, s_m\}$，整个集群的密码服务负载上限分布表示为矩阵：

$$\boldsymbol{A}=\begin{Bmatrix} a_{11},a_{12},\cdots,a_{1j} \\ a_{21},a_{22},\cdots,a_{2j} \\ \vdots \\ a_{i1},a_{i2},\cdots,a_{ij} \end{Bmatrix};\ i=1,2,\cdots,n;\ \ j=1,2,\cdots,m \tag{1}$$

式中：n 为集群内服务器数量，m 为系统中密码服务最大项数。考虑到各服务器支持的密码服务项数不同，a_{ij} 的值表示第 i 台服务器第 j 项服务的最大负载值。

定义 n 台主机的 m 项密码服务的负载值矩阵为：

$$\boldsymbol{P}=\begin{Bmatrix} p_{11},p_{12},\cdots,p_{1j} \\ p_{21},p_{22},\cdots,p_{2j} \\ \vdots \\ p_{i1},p_{i2},\cdots,p_{ij} \end{Bmatrix};\ i=1,2,\cdots,n;\ \ j=1,2,\cdots,m \tag{2}$$

将 $\boldsymbol{P}$ 矩阵进行归一化处理 $c_{ij}=\dfrac{p_{ij}}{a_{ij}}$，得到矩阵：

$$\boldsymbol{C}=\begin{Bmatrix} c_{11},c_{12},\cdots,c_{1j} \\ c_{21},c_{22},\cdots,c_{2j} \\ \vdots \\ c_{i1},c_{i2},\cdots,c_{ij} \end{Bmatrix};\ i=1,2,\cdots,n;\ \ j=1,2,\cdots,m \tag{3}$$

式中：$0\le c_{ij}\le 1$，c_{ij} 表示第 i 台服务器中第 j 项密码服务的归一化负载值。$C_j=\{c_{1j}, c_{2j}, \cdots, c_{nj}\}^{\mathrm{T}}$ 表示第 j 项密码服务在集群中的利用率。为最大程度地释放底层算力，可将密码资源利用率设为集群负载均衡的主要影响因素，那么可由式（3）再对 $\boldsymbol{C}$ 矩阵进行标准化处理：

$$Q_{ij}=\frac{c_{ij}-\min\{C_i\}}{\max\{C_i\}-\min\{C_i\}} \tag{4}$$

式中：$\boldsymbol{C}_i$ 为 $\boldsymbol{C}$ 矩阵中的第 j 列的列向量，$\boldsymbol{Q}_{ij}$ 为标准化后矩阵中的元素，组成新的标准化矩阵 $\boldsymbol{Q}$，如下所示：

$$\boldsymbol{Q}=\begin{Bmatrix} q_{11},q_{12},\cdots,q_{1j} \\ q_{21},q_{22},\cdots,q_{2j} \\ \vdots \\ q_{i1},q_{i2},\cdots,q_{ij} \end{Bmatrix};\ i=1,2,\cdots,n;\ \ j=1,2,\cdots,m \tag{5}$$

计算第 j 项资源状态指标下，第 i 台服务器的特征比重：

$$b_{ij}=\frac{q_{ij}}{\sum_{j=1}^{m}q_{ij}},0\le b<1 \tag{6}$$

对于某项资源状态指标 q_{ij}，它的差值越大，此项资源状态的信息熵值就越小；指标信息熵值的计算公式为：

$$e_j=-k\sum_{i=1}^{n}b_{ij}\ln b_{ij};\ j=1,2,\cdots,m \tag{7}$$

式中：k 为调节系数，$k=\dfrac{1}{\ln n}$。

考虑到在计算密码设备的特征比重时会出现 0 的情况，进而导致计算熵值时出现 ln0，影响后续计算结果，因此，在计算信息熵值时添加集群的密码服务分布矩阵 $\boldsymbol{C}$：

$$e_j=-\frac{\sum_{i=1}^{n}c_{ij}(b_{ij}\ln b_{ij})}{\ln\sum_{i=1}^{n}c_{ij}};\ \ j=1,2,\cdots,m \tag{8}$$

接着引入熵冗余系数 $d_j=1-e_j$。由此可以得到各项密码资源状态的权重：

$$w_j=\frac{d_j}{d_1+d_2+\cdots+d_m} \tag{9}$$

并且 $\sum_{j=1}^{m}w_j=1$，最后，计算当前服务器的服务能力评价系数 $E_i=\sum_{j=1}^{m}w_jb_{ij};\ i=1,2,\cdots,n$。

2.2 负载信息传播模型

本文采用去中心化的负载信息传播模型，每个服务节点维护一个全局负载分布视图，服务节点之间利用 Gossip 协议传递密码服务负载信息。考虑到信息传播时的网络开销，规定信息转发次数的上限。保证网络效率的同时，尽量让每个节点接近真实的全局负载分布情况。

每个服务节点均维护整个集群的密码服务负载信息。每个节点的负载信息都包含 4 个数据项，服务节点 NodeIP、时间戳 Timestamp、密码服务负载矩阵 p_i 和密码服务负载上限矩阵 $\boldsymbol{a}_i$。

为保证全局负载分布情况的实时性，每个服务节点需要实时更新其路由表，并通过 Gossip 协议将负载消息转发给其他节点。考虑到网络效率，将消息被其他节点转发次数的上限定为 6 次。同时，在节点负载信息 4 个数据项的基础上，再加入转发次数标识 Forward。负载信息的传播流程具体如图 1 所示。

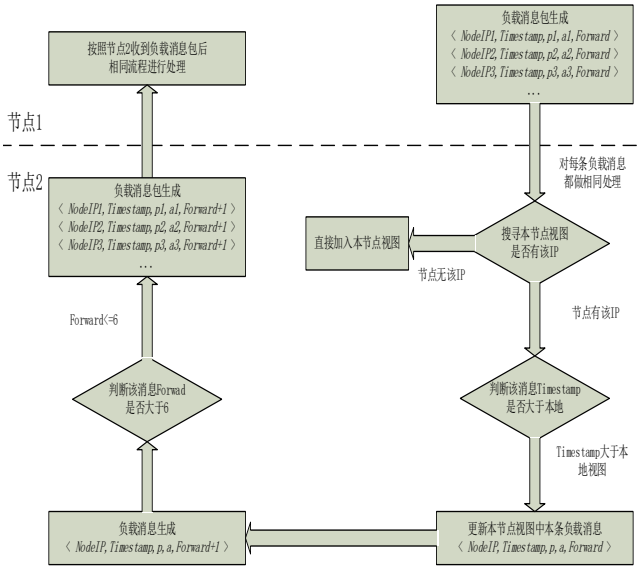

图 1 负载信息传播流程图

2.3 基于前馈神经网络的负载预测模型

考虑到各节点之间的密码服务算力可能存在差异，且常用的几种密码算法工作模式所需资源均与对应参数强相关，为更合理地分配算力资源，引入前馈神经网络来评估当前业务对当前节点的密码服务资源需求度。

定义系统各算法工作模式参数矩阵集合：

$$U=\begin{Bmatrix}u_{11},u_{12},\cdots,u_{1k}\\u_{21},u_{22},\cdots,u_{2k}\\\vdots\\u_{j1},u_{j2},\cdots,u_{jk}\end{Bmatrix};\ j=1,2,\cdots,m;\ \ k=1,2,\cdots,o \tag{10}$$

式中：u_{jk} 表示第 j 项密码服务中第 k 个参数的负载值。考虑到各服务器支持的密码服务项数不同，定义 $\boldsymbol{A}_i=(a_{i1}, a_{i2}, \cdots, a_{im})$，$a_{ij}$ 的值可能为 0 或者 1，表示当前服务器支持的密码服务项数。

将矩阵 $\boldsymbol{A}_i$ 进行对角化处理得到：

$$\boldsymbol{B}=\begin{pmatrix}a_{i1},0,\cdots,0\\0,a_{i2},\cdots,0\\\vdots\\0,0,\cdots,a_{im}\end{pmatrix} \tag{11}$$

矩阵 $\boldsymbol{B}$ 为 $m\times m$ 的矩阵，令 $\boldsymbol{C}=\boldsymbol{B}\times\boldsymbol{U}$，并判断 $\boldsymbol{C}$ 是否等于 $\boldsymbol{U}$，若不相等则直接根据策略跳转节点，否则表示当前节点具备任务 $\boldsymbol{U}$ 所需的所有算法模式并进入前馈神经网络进行负载预测。

在前馈神经网络中，每个节点（神经元）接收来自上一层节点的输入，并经过线性变换和激活函数处理之后，将结果传递到下一层。隐藏层和输出层中的节点具有权重和偏置，通过学习算法来调整这些参数，使神经网络能够学习到输入数据特征并进行有效预测。

本文采用三层前馈神经网络结构，如图 2 所示。

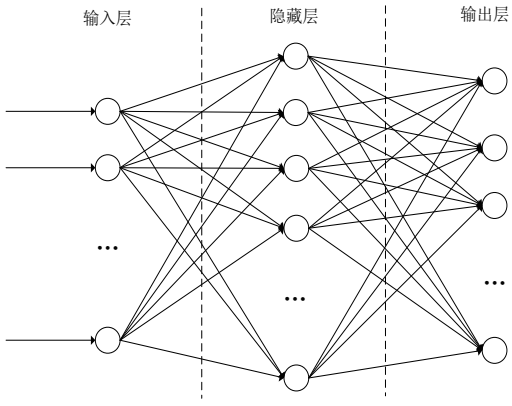

图 2 前馈神经网络结构图

在输入层中，本文将算法工作模式参数矩阵和当前节点负载矩阵作为 $j\times k+m$ 个输入单元。对于输出层图 2 前馈神经网络模块设置 m 个神经元，用来输出当前节点各类密码服务资源负载。隐藏层采用单隐层，设置神经元个数 h。其中输入层到隐藏层关系可用式（12）表示，隐藏层自身的输出用式（13）表示，隐藏层到输出层的关系用式（14）表示。

$$d_o=\sum_{i=1}^{j\times k+m}w_{oi}x_i+\theta_o, i=1,\cdots j\times k+m; o=1,\cdots,h \tag{12}$$

$$z_o=f\left(d_o\right), o=1,2,\cdots,h \tag{13}$$

$$p_m=f\left(\sum_{j=1}^{h}w_{jm}z_o+\theta\right), j,o=1,2,\cdots,h \tag{14}$$

式中：x_i 表示输入层的输入值，w_{oi} 表示输入层到隐藏层之间的权重，θ_o 表示隐藏层神经元的阈值，d_o 表示隐藏层的输入值；z_o 表示隐藏层的输出值；w_{jm} 表示隐藏层到输出层之间的权重，θ 表示输出层神经元的阈值，p_m 表示预测的第 m 项密码服务资源利用率；$f(x)$ 为激活函数，这里选用 sigmoid 函数：

$$f\left(x\right)=\frac{1}{1+e^{-x}} \tag{15}$$

可以得到第 i 个节点预测的资源利用率，表示为 $p_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$。

2.4 调度策略

针对在线业务高效调度、资源动态配置的需求，在基于熵权法的差异化密码服务评价方法的基础上，利用去中心化的负载信息传播模型同步各节点信息，以此为依据生成密码

业务调度策略。

首先通过前馈神经网络预测该业务的负载需求度，并采用基于熵权法的差异化密码服务评价方法得出该节点的服务能力评价系数，结合去中心化的负载信息传播模型同步节点负载信息，在此基础上生成密码业务调度策略，扩展了密码服务能力，解决了密码资源的动态扩展问题，满足了密码服务差异化需求。

3 系统实现

3.1 系统模型

基于本文提出的分布式按需提供密码服务调用方案，搭建密码按需服务系统模型，整体架构如图 3 所示。该系统对终端侧提供接入认证、数据安全存储等密码业务服务，并根据不同密码服务需求动态调度、管理密码设备。

（1）终端应用侧

终端应用侧主要部署直接提供给用户相关应用服务的终端，比如 PC 终端、手持平板终端、便携笔记本终端等。终端可直接访问后台服务区，调取应用需要的服务。比如应用需要认证服务，可直接访问认证服务器，需要安全存储服务，可访问存储服务器。

（2）后台服务区

后台服务区主要部署了各种类型的应用服务器，对上可支撑各类可灵活的前端应用，对下可按需调用密码服务区的签名、验签、哈希、加解密、证书操作等底层密码服务。

（3）密码服务区

密码服务区部署各类高性能密码服务器，其中内置各类高速 PCIE 密码卡，可提供签名、验签、哈希、加解密等密码服务，同时具备高度的可扩展性。管理员可根据后台服务区需要，动态接入新的密码服务器。

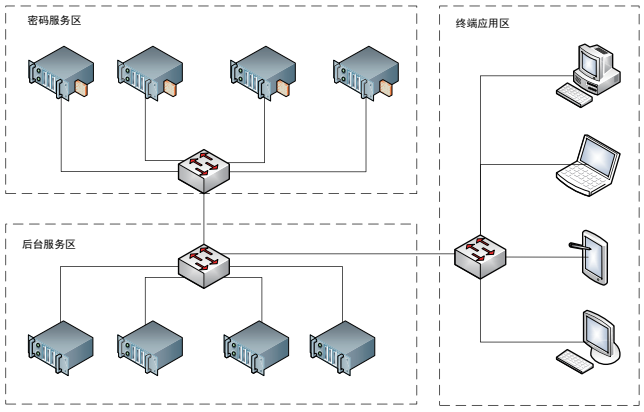

图 3 系统模型图

3.2 系统运行策略

分布式按需提供密码服务调用方案的作业调度策略步骤如下。

（1）业务请求发起

终端应用侧发起密码业务请求，访问到后台服务区。后台服务区处理非密码业务请求，并根据业务类型生成签名验签、加密解密等底层密码服务访问请求，同步访问密码服务区。

（2）密码服务请求接收

密码服务区的服务节点首先解析密码服务请求，获得算法工作模式参数矩阵 $\boldsymbol{U}$，通过公式 $\boldsymbol{C}=\boldsymbol{B}\times\boldsymbol{U}$ 判断当前节点是否具备任务所需算法模式，如具备，则进行下一步；如不具备，就转到（5）密码服务请求转发。

（3）密码服务负载预测

将当前节点资源利用率 p_i 与当前任务的参数矩阵 $\boldsymbol{U}$ 作为神经网络的输入，预测出加入当前任务后的资源利用率 p_i'。

（4）密码服务能力评估

通过资源利用率 p_i'，利用基于熵权法的差异化密码服务评价方法计算出密码设备的服务能力评价系数。如果当前评价系数在路由队列里是最高的，则选择当前节点完成任务，否则转到下一步。

（5）密码服务请求转发

在当前密码设备的路由队列中检索是否还有可选择的密码设备，若没有则转到（5）密码服务请求转发等待路由队列的更新，否则将该任务请求转发到路由队列中服务能力评价系数最高的节点，并继续从（2）密码服务请求接收重复流程。

4 系统测试与分析

系统试验环境部署 5 台服务器密码机，作为密码计算节点，其中 3 台服务器密码机的密码计算单元是剩余 2 台服务器密码机密码计算单元数量的两倍；5 台通用服务器作为系统的测试节点。其中每个计算节点包括两个 64 核 2.1 GHz 的 CPU，6 个 32 GB 的内存和 2 个万兆网口用于业务交互，2 个千兆网口用于管理信息交互；5 台通用服务器模拟业务系统对集群进行测试。

实验中共提供对称加解密、非对称加密、非对称解密、签名、验签、哈希 6 种密码服务，应用端的业务请求数按 50 的倍数增加，每个服务请求从 6 种密码服务组合中随机选择多种生成请求。业务请求增加时保持同样比例的密码服务类型，密码服务调度策略分别采用本文的方案、中心化按需调度方案和分布式贪婪策略调度方案，记录单位时间的服务请求数量。为了更加客观地模拟实际环境，应用端同时发出请求，3 种调度策略对比时其请求的密码服务组合种类和数量完全相同，分别独立运行 20 次后取平均值，实验结果如图 4 所示。

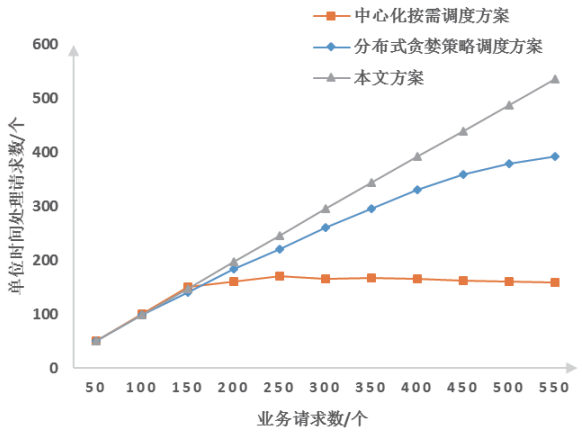

图 4 单位时间服务请求数对比图

由图 4 可以看出，在业务请求数较低时，三种方案在单位时间处理请求数差异不大。但随着业务请求数的增长，中心化按需处理的方案的单位时间处理请求数很快就达到了峰值，能继续保持增长的为本文方案和分布式贪婪策略调用方案。在业务请求数进一步增长时，由于本文方案采用按需调度策略，单位时间处理请求数要明显优于分布式贪婪策略调度方案。

5 结语

本文提出了一种分布式按需提供密码服务调用的方案。利用分布式负载模型，在业务输入端进行分流，提升了高并发场景下的业务处理性能瓶颈。同时，使用基于前馈神经网络的负载预测模型，并结合基于熵权法的差异化密码服务评价方法，对节点负载能力进行预测与分析，可以在复杂多变的集群环境下更为高效地使用集群的密码算力。

为验证本文方案效能，通过搭建试验环境进行了对比测试。测试结果表明，在相同业务负载条件下，本文方案具有更高的业务负载上限和更优的业务负载效率。

在后续工作中，需要重点研究负载信息传播模型和预测模型，提升信息传播的效率，并提高负载预测的准确度。

参考文献：

[1] 李建军，郁滨，陈武平 . 面向服务组合的密码服务调度智能优化研究 [J]. 通信学报，2013,34(S1):216-222.

[2] 唐月婷，蒋朝惠 . 一种基于 SDN 的服务器负载均衡方案 [J]. 通信技术，2018,51(5):1117-1122.

[3]AROCA J A, MOSTEIRO M A, THRAVES C, et al.Power-efficient assignment of virtual machines to physical machines[J].Future generations computer systems, 2016, 54: 82-94.

[4]DUAN H, CHEN C, MIN G, et al.Energy-aware scheduling of virtual machines in heterogeneous cloud computing systems[J].Future generation computer systems, 2017,74:142-150.

[5]MAIO V D, KECSKEMETI G, KECSKEMETI G, et al.Modelling energy consumption of network transfers and virtual machine migration[J].Future generation computer systems, 2016, 56:388-406.

[6]GRANDL R, CHOWDHURY M, AKELLA A, et al.Altruistic scheduling in multi-resource clusters[EB/OL].(2016-11-02)[2024-02-19].https://dl.acm.org/doi/10.5555/ 3026877.3026884.

[7] 杨婷，万良，马绍菊，等 . 一种自适应权值最小负载的 LVS 集群负载均衡算法 [J]. 通信技术，2017,50(4):741-745.

[8]LIANG Y, LAN Y.TCLBM:a task chain-based load balancing algorithm for microservices[J].Tsinghua science and technology, 2021,26(3):251-258.

[9] 李鑫，张沪寅，吴笛，等 . 一种利用分布式遗传算法的 P2P 负载均衡方法 [J]. 武汉大学学报 (信息科学版), 2013, 38(3): 315-318+343.

[10]LI F, JI H, ZHOU H, et al.A cryptographic resource management framework and dynamic migration method based on virtualization[C]//2021 7th International Conference on Computer and Communications.Piscataway: IEEE,2021:560-564.

[11] 寇文龙，张宇阳，李凤华，等 . 密码服务资源按需高效调度方案 [J]. 通信学报，2022,43(6):108-118.

【作者简介】

王曦（1992—），男，四川华蓥人，硕士，工程师，研究方向：信息安全与保密通信。

赵涔伶（1985—），女，四川成都人，硕士，工程师，研究方向：信息安全与保密通信。

周波（1992—），男，四川会理人，硕士，工程师，研究方向：信息安全与保密通信。

杜薇（1983—），女，四川成都人，硕士，高级工程师，研究方向：信息安全与保密通信。

（收稿日期：2024-04-22）