

SR-IOV 密码设备中断传输过程建模

孙磊, 李帅, 郭松辉

(信息工程大学, 河南 郑州 450001)

摘要: SR-IOV 密码设备在虚拟化环境下执行运算时会产生大量 I/O 中断, 导致 CPU 在 Root 模式与 Non-Root 模式之间频繁切换, 带来巨大的系统性能开销, 影响 SR-IOV 密码设备的运算性能。针对该问题, 对 SR-IOV 密码设备 I/O 中断进行建模分析, 根据密码任务先到先服务的规则构建了 M/M/1 排队模型, 分析了影响系统性能的关键因素, 并通过仿真和实验测试验证了模型的有效性, 最后对系统性能进行了测试与分析。结果表明, 该模型能够定量分析中断频率对中断响应时间和系统队长的影响。

关键词: 中断; SR-IOV; 密码设备; 排队模型; 性能

中图分类号: TP302.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019007

Modeling the interrupt transmission process of SR-IOV cryptographic device

SUN Lei, LI Shuai, GUO Songhui

Information Engineering University, Zhengzhou 450001, China

Abstract: The SR-IOV cryptographic device generates a large number of I/O interrupts when performing operations in a virtualized environment, causing the CPU to frequently switch between the Root mode and the Non-Root mode, which brings huge system performance overhead and affects the operational performance of SR-IOV cryptographic device. Aiming at this problem, the I/O interrupt of SR-IOV cryptographic device was analyzed, and a M/M/1 queuing model according to the cryptographic task first-come-first-served rules was constructed. What's more, the key factors affecting system performance were analyzed, and the validity of the model via simulation and experiment was verified, and finally the system performance was tested. The results show that the model can quantitatively analyze the impact of the interrupt frequency on the interrupt response time and system queue length.

Key words: interrupt, SR-IOV, cryptographic device, queuing model, performance

收稿日期: 2018-12-09; 修回日期: 2018-12-26

通信作者: 李帅, 2650536170@qq.com

基金项目: 国家重点研发计划基金资助项目(No.2016YFB0501900)

Foundation Item: The National Key R & D Program of China (No.2016YFB0501900)

论文引用格式: 孙磊, 李帅, 郭松辉. SR-IOV 密码设备中断传输过程建模[J]. 网络与信息安全学报, 2019, 5(1): 56-65.

SUN L, LI S, GUO S H. Modeling the interrupt transmission process of SR-IOV cryptographic device[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 56-65.

1 引言

近年来,云计算凭借其强大的计算和存储能力逐渐在产业界得到广泛应用^[1]。随着云计算的快速发展,其应用也逐渐在军事、电子商务和电子政务等领域得到推广,而同时云计算也面临为敏感信息提供机密性、完整性和真实性等保护的迫切需求。通过部署密码服务器,利用虚拟化技术为用户提供密码运算服务,是目前广泛使用的密码服务保障模式^[2]。

密码服务器通过外接密码设备为用户提供密码运算服务,密码设备处理密码任务不仅要求运算的正确性,还要求任务处理的实时性^[3]。在虚拟化环境下,由虚拟密码机(VCM, virtual cipher machine)(为用户提供密码服务的虚拟机)^[4]发出的密码运算请求以中断的方式通知密码设备,然而在整个中断传输的过程中存在较大延迟,这是由于虚拟机监控器(VMM, virtual machine monitor)会截获相应的中断,触发 VM-exit 造成的。单根 I/O 虚拟化技术(SR-IOV, single-root I/O virtualization)^[5]是一种硬件辅助虚拟化技术,该技术借鉴 Passthrough I/O 传输方式^[6],在数据传输过程中绕过 VMM,并通过输入/输出内存管理单元(IOMMU, input/output memory management unit)减少了存储保护和地址转换的开销,大大提高了传输效率^[7]。然而,虚拟中断请求仍然会被 VMM 截获,其传输过程造成多次上下文切换,使在中断密集时,密码设备不能及时处理密码运算任务,降低了密码运算的效率。而且,当云中用户对加密服务的请求在同一时间过多时会产生大量不可预测的中断请求,导致密码设备外部中断请求过多,严重影响了密码设备处理密码运算的能力,增大了系统开销^[8]。

针对 SR-IOV 设备中断的问题,国内外学者进行了大量研究。Dong 等^[9]在 2010 年指出了

SR-IOV 中断引起的性能降低问题,在对 SR-IOV 中断优化的过程中,上海交通大学管海兵团队先后提出了中断聚集方法^[10]、基于事件的轮询方法^[11]和一种自适应中断频率控制方法^[12],这 3 种方法分别从优化中断频率和消除 VM-exit 入手来提高系统性能。然而,中断聚集方法和自适应中断频率控制方法需要考虑多方面因素,因为中断聚集意味着每次中断带来的数据量较大,可能会导致数据丢失,且中断聚集引起的中断频率的减少可能会带来更高的延迟,这在高速网络传输过程中是非常严重的问题。而采用基于事件的轮询方法是以虚拟中断注入作为轮询起点,这是一条更长的代码路径,会造成额外开销。国外学者 Gordon 等^[13]提出了一种更少中断退出的机制(ELI, exit-less interrupt),该机制采用软件模拟的方式在客户虚拟机内建立影子中断描述符表(IDT, interrupt description table),可实现客户机直接处理中断,但 ELI 只允许影子 IDT 直接处理已经分配的设备中断,其他中断仍需要主机的介入,云环境下中断请求复杂多样,该方法显然具有一定的局限性。Tu 等^[14]提出了一种直接中断传输的方法(DID, direct interrupt delivery),该方法通过清除虚拟机控制结构中的外部中断控制位来禁止 VM-exit,可能会导致中断的错误处理。从虚拟密码设备的角度来说,这种做法会导致密码运算错误,是不可取的。

研究影响 SR-IOV 密码设备的性能问题必须要考虑密码任务的特点,本文以单台密码服务器为例,针对虚拟化环境下 SR-IOV 密码设备频繁产生中断影响运算性能的问题,根据密码任务先到先服务的规则,利用排队论的知识建立了 M/M/1 模型,分析了影响 SR-IOV 密码设备密码运算性能的关键因素,并通过仿真和实验对比验证了模型的有效性,最后对系统性能进行了测试。

足密码任务实时性的要求。

2.2 关键问题

由 2.1 节的分析可知, 用户发出的密码运算请求以中断的方式通知密码设备上相应的寄存器, 交由密码运算单元处理密码任务。在虚拟化环境下, 由虚拟密码机发出的密码运算请求同样以中断的方式通知密码设备, 然而在整个中断传输的过程中有相应的延迟, 这是由于 VMM 会截获相应的中断, 触发 VM-exit 事件造成的。VMM 截获中断信号之后将中断注入主机内核, 主机内核调用相关的函数接口将密码请求任务交给密码设备, 密码设备执行完密码任务后生成一个完成信号, 该信号返回给虚拟机的过程中再次被 VMM 截获, 触发 VM-exit 事件, 引发 EOI 写操作。整个中断传输的过程造成多次上下文切换, 当中断频率过大时, 频繁的上下文切换使 cache 污染的概率大大提高^[9], 严重影响密码设备运算性能。物理环境下和虚拟环境下的中断处理过程如图 2 和图 3 所示。

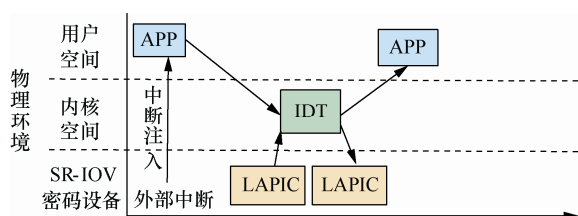


图 2 物理环境下的中断处理过程

由图 2 和图 3 对比分析知, 物理环境下的中

断处理过程造成了两次上下文切换, 且不存在虚拟机监控器的参与; 而虚拟环境下的中断处理造成了 4 次上下文切换, 且每次 VM-exit 事件均被 VMM 截获, 开销比物理环境下大得多。如果将虚拟环境下中断的处理过程分成虚拟机处理中断和 VMM 介入两部分, 在运行 Netperf 工作流下, 实验测得两部分消耗的 CPU 周期中, 由 VMM 介入所消耗的 CPU 周期高达 86%^[16]。而且, 密码算法的操作序列比较长, 当采用密码算法对一段数据进行加密时, 一般具有大量重复的操作。由于 VMM 截获中断的开销较大, 当虚拟化环境下的中断频率过多时, 会造成更大的开销, 当大量的中断引发中断嵌套时, 甚至会加解密失败, 严重影响了密码设备处理密码运算的效率。Intel Corporation DH895XCC Series QAT 密码设备考虑到虚拟机中断带来的巨大开销, 采用基于事件的轮询模式——“Epoll 模式”处理响应, 但该模式只能在用户空间中使用, 内核空间部分依然利用中断模式, 如果内核中断有延迟, 则会在向用户空间交付事件时出现相应的延迟^[11]。因此, 在密码设备处理密码运算任务的过程中, 中断的发生是必然的, 处理中断所引起的系统开销也是不可避免的, 而系统开销的大小取决于中断带来的延时。在上述的分析中, 造成中断延时的原因主要是中断处理过程中 VMM 的介入和高中断频率。

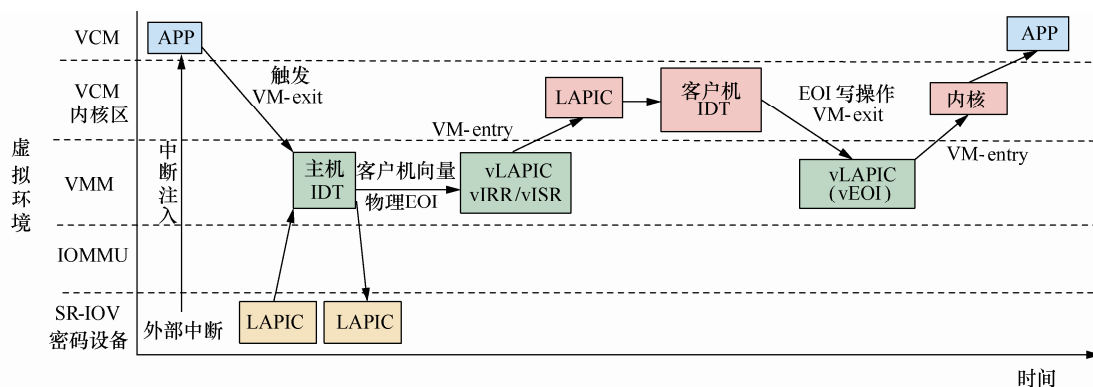


图 3 虚拟环境下的 I/O 中断处理过程

3 模型建立与分析

3.1 模型建立

在单个服务器上，SR-IOV 密码设备中断传输过程如图 4 所示，主要包括 SR-IOV 密码设备、虚拟密码机、VMM 和中断请求队列。其中，密码设备采用 SR-IOV 技术将单个物理设备呈现为一个 PF 和若干 VF。在实际使用时，把每个 VF 分配给每一个虚拟密码机，虚拟密码机通过 VF 获取密码设备资源，完成密码运算操作。由于 VF 之间相互隔离，因此每台虚拟密码机执行密码运算时互不影响。但由于虚拟密码机共享硬件资源，当同一时间内，虚拟密码机发出大量中断请求时，会造成主机不能及时处理中断请求，从而形成中断请求队列。在中断请求队列中，密码运算类中断请求具有同等优先级，因此队列中的中断请求按照先到先服务的规则进行排序。密码设备处理完密码运算后生成一个 EOI 信号交由 VMM 处理，处理完成后注入 VCM，最终 VCM 恢复正常运行。

在 SR-IOV 密码设备中断传输过程中，两个相邻中断请求的时间间隔具有无记忆性，且每个中断请求之间相互独立，实际上，系统中中断请求的到达过程具有马氏性，且两个相邻中断请

求时间间隔服从指数分布。中断请求进入排队系统后，系统处理每个中断请求的时间是独立同分布的指数随机变量，且服从指数分布。上述中断请求时间间隔和系统处理每个中断请求的时间所满足的概率分布符合排队论的基本条件^[17]，且队列中的中断请求按照先到先服务的规则进行排序，则针对单个服务器，密码服务系统中每个虚拟密码机的中断请求处理过程构成了 M/M/1 排队模型。

3.2 模型分析

假设密码服务系统中中断请求的平均到达率为 λ ，系统处理每个中断请求的平均服务率为 μ 。考虑到密码服务系统中中断请求的随机性，取中断请求时间间隔的平均值为 T_b ，则系统任务的平均到达率 $\lambda = \frac{1}{T_b}$ ，即系统中中断请求

频率。假设系统中中断请求频率为 I ，则 $\lambda = I$ 。取系统处理每个中断请求的平均处理时间为 T ，则中断的平均服务速率为 $\mu = \frac{1}{T}$ 。假设 $N(t)$

表示 t 时刻系统中中断请求队列长度，其中包括正在处理的中断以及队列中的中断。对 M/M/1 排队模型来说， $\{N(t), t \geq 0\}$ 是一个时间参数连续的马氏链，实际上是一个生灭过程，其 Q 矩阵为

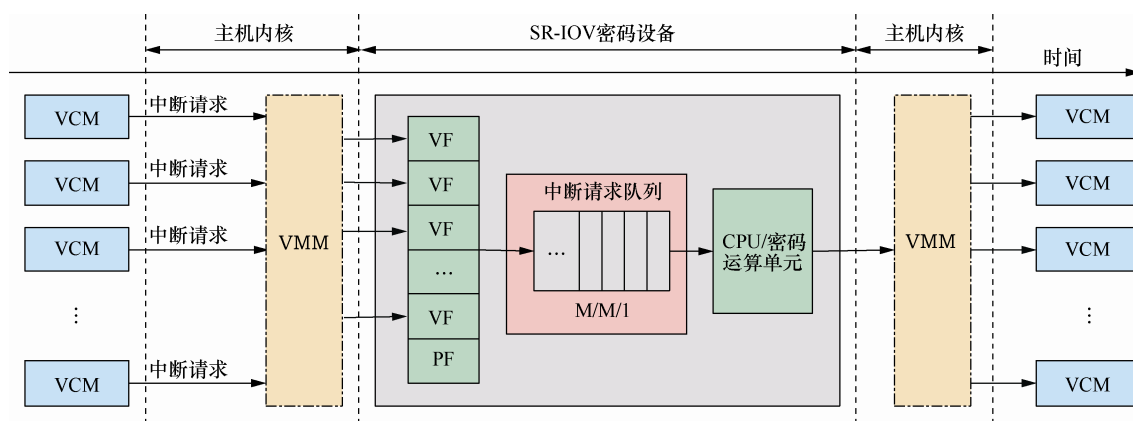


图 4 SR-IOV 密码设备中断传输过程

$$Q = \begin{pmatrix} -\lambda & \lambda & & & \\ \mu & -(\lambda + \mu) & \lambda & & \\ & \mu & -(\lambda + \mu) & \lambda & \\ & & \ddots & \ddots & \ddots \\ & & & \ddots & \ddots \end{pmatrix}$$

根据 Q 矩阵, 可画出 $\{N(t), t \geq 0\}$ 的状态转移图, 如图 5 所示。

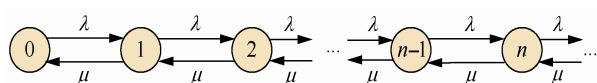


图 5 系统中断请求队长状态转移图

则系统的稳态队长的分布为

$$p_k = \lim_{t \rightarrow \infty} p_k(t) = (1 - \rho) \rho^k$$

当 $k = n$ 时

$$p_n = (1 - \rho) \rho^n$$

其中, ρ 为系统服务强度, 且 $\rho = \frac{\lambda}{\mu} = \frac{T}{T_b}$ 。

当 k 取 0 时, 得出系统处于空闲状态的概率为

$$p_0 = 1 - \rho = 1 - \frac{\lambda}{\mu} = 1 - \frac{T}{T_b}$$

则系统处于繁忙状态的概率为

$$p = 1 - p_0 = \frac{T}{T_b} = TI$$

由 little 公式^[18], 系统的平均任务数为

$$L_s = \sum_{n=0}^{\infty} n p_n = \frac{\rho}{1 - \rho} = \frac{T}{T_b - T} = \frac{1}{1 - TI} - 1$$

在密码服务系统中, 系统的平均中断响应时间反映了密码设备处理中断请求的效率, 它等于从虚拟密码机发出中断请求开始到 SR-IOV 密码设备接收到中断请求并进入中断处理程序的时间。在 SR-IOV 密码设备中断传输过程中, 这个时间可分为两部分: 中断请求的排队等待时间和中断请求在系统中的传输时间。假设 T_q 为中断请求的排队等待时间, T_t 为

中断请求在系统中的传输时间, 则系统的平均中断响应时间可表示为

$$T_r = T_q + T_t = \frac{1}{\frac{\mu}{1 - \rho}} = \frac{T}{1 - \frac{T}{T_b}} = \frac{T}{1 - TI}$$

根据 little 公式, 中断请求队列的平均长度 L_q 为

$$L_q = \lambda T_q = \frac{T_q}{T_b} = T_q I$$

在上述性能参考指标中, 系统服务强度 ρ 一般情况下小于 1, 即系统处理每个中断请求的平均处理时间 T 小于中断请求时间间隔 T_b ; 若 ρ 大于 1, 显然系统不能及时处理中断请求, 且随着时间的推进, 系统中断请求的队长将趋于无限; 若 ρ 等于 1, 则系统一直处于繁忙状态, 即系统每接收到一个中断请求信号就马上处理, 处理完毕后又立即处理下一个中断请求信号, 但中断响应都有相应的延时, 随着时间的推进, 系统中断请求的队长也将趋于无限。显然, 在 SR-IOV 密码设备中断传输过程中, ρ 大于等于 1 的情况是不希望发生的, 那么 T 一定不能超过 T_b , 且 $I = \frac{1}{T_b}$, 即控制系统中断请求频率 I 不能过大。

在 SR-IOV 密码设备中断传输过程中, 系统的中断响应时间直接体现了密码设备处理密码运算的效率。在上述性能参考指标中, 系统的平均中断响应时间 T_r 由中断请求排队等待时间 T_q 和中断请求传输时间 T_t 组成, 可通过减少 T_q 和 T_t 降低系统的中断响应时间。减少 T_q 的本质是增大 T_b , 即降低 I 。由第 2 节分析可知, 减少中断请求传输时间 T_t 要从 VMM 入手, 即尽可能避免 VMM 截获中断。因此, 要提高 SR-IOV 密码设备密码运算性能, 需从降低系统中断请求频率和减少 VMM 介入入手。

4 验证与分析

本文采用软件仿真和实验测试两种方式验证模型的有效性,并对性能特征进行分析。软件仿真使用 Matlab_2016a 建立模型,实验环境如下。主机和虚拟密码机操作系统均为 CentOS-7-x86_64-1511,内核版本为 Linux 3.10.0-327.el7.x86_64,处理器为 Intel(R) Xeon(R) CPU E5-2620 v3@2.40 GHz, CPU 核心数为 12 核,内存大小为 128 GB,支持 SR-IOV 技术,每台虚拟密码机均分配一个 vCPU 和 2 048 MB 内存,密码设备为 Intel Corporation DH895XCC Series QAT。

4.1 模型有效性验证

SR-IOV 密码设备的 VF 自身支持中断频率上限的设置,实验中本文分别设置 VF 中断频率上限为 1 000、2 000、3 000、4 000、5 000、6 000、7 000、8 000、9 000 和 10 000,测试了单个虚拟密码机在相应设置下的中断响应时间,测试结果与仿真结果进行对比,结果如图 6(a)所示。为了测试整个系统的运行队列长度,本文分别运行 1 台、2 台、4 台、8 台和 16 台虚拟密码机,测试系统运行队列长度,并对仿真结果进行对比,结果如图 6(b)所示。图 6 表明,实验结果与仿真结果曲线走势相同,模型有较高的有效性。

4.2 系统性能测试

本节选取对称加密算法 AES128 作为实验对象,以密码算法的加密速度作为虚拟密码机性能参考指标,基于 cryptodev 加密框架^[18]发送和接收相关指令,实现虚拟密码机与密码设备的通信,获取相应的密码服务。该加密框架可以测试虚拟密码机密码运算速度,其中包含 AES128 等加密算法。系统性能的各项指标由 Linux vmstat 命令获得,该命令可获得给定时间间隔内系统的状态值,包括系统队列长度、系统中断频率、系统

上下文切换次数、系统 CPU 时间和用户 CPU 时间等。其中,系统队列长度表示当前系统正在运行的进程数目,系统中断频率表示每秒 CPU 的中断次数,系统上下文切换次数主要反映调用系统函数的繁忙程度,系统 CPU 时间和用户 CPU 时间主要反映系统 I/O 操作的繁忙程度。下面分别对单台虚拟密码机和多台虚拟密码机进行性能测试。

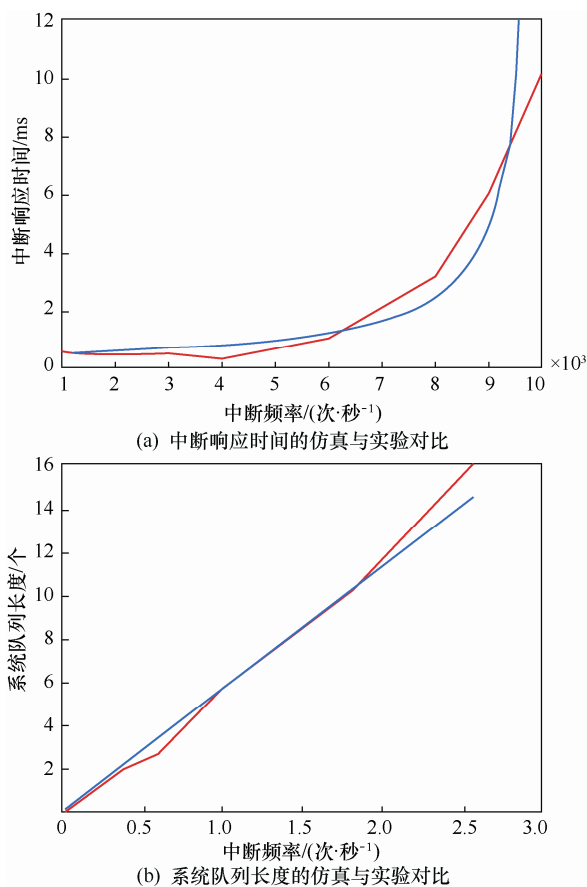


图6 模型有效性验证

首先对一台虚拟密码机进行测试,在分别运行 1 个任务、2 个任务、4 个任务和 8 个任务的情况下,测试虚拟密码机在输入加密数据分组大小从 64 byte 变化到 65 536 byte 11 次的加密速度,反复测试 10 次求取平均值,测试结果如图 7(a)所示。图 7(a)的测试显示了虚拟密码机处理单个密码任务时, AES128 算法对接收到的不同加密字节块

大小加密速度的变化趋势。从实验结果中可以看出,加密字节在 16 384 之前,虚拟密码机加密速度一直在增大,当加密字节为 16 384 时,虚拟密码机加密速度达到最大,当加密字节继续增大时,虚拟密码机加密速度基本无变化甚至出现降低的趋势。使用 `vmstat` 相关命令获取系统实时中断频率、上下文切换次数和系统 CPU 时间,记录 11 次采样结果。图 7(b)显示了虚拟密码机分别运行 1 个任务、2 个任务、4 个任务和 8 个任务时的每秒中断频率,其平均值分别为 1 065、1 126、1 173 和 1 323,说明随着任务量增加,系统中断频率不断增大。图 7(c)显示了虚拟密码机分别运行 1 个任务、2 个任务、4 个任务和 8 个任务时系统的上下文切换次数,且系统的平均上下文切换次数为 299、345、391 和 451,说明系统任务量越大,系统上下文切换次数越多。图 7(d)显示了虚拟密码机分别运行 1 个任务、2 个任务、4 个任务和 8 个任务时的系统 CPU 时间,该值基本保持在 85%以上。其中运用 `vmstat` 命令测试得

出的系统 CPU 时间越长,表明系统调用时间越长,如频繁的 I/O 操作会导致较高的系统 CPU 时间,这也说明了 AES128 加密操作属于 I/O 密集型的操作。综合图 7,对于单台虚拟密码机来说,密码任务越多,运算性能越低,这不仅是由于每个密码任务平分物理硬件资源,任务增加带来的中断频率增大以及上下文切换次数增大也是导致运算性能降低的主要因素。因为对于同一类密码任务来说,多个任务的加密速度之和总是小于一个任务的加密速度,且任务越多差值越大。

为了测试多台相同配置的虚拟密码机同时工作时带来的性能开销,分别对 1 台、2 台、4 台、8 台和 16 台虚拟密码机同时循环执行 AES128 加密运算,用 `vmstat` 命令每 2 s 进行一次采样,记录 15 次采样结果,筛选出系统运行队列长度、系统每秒中断频率、系统每秒上下文切换次数和用户 CPU 时间,具体结果如图 8 所示。由图 8(a)和图 8(b)可明显看出,当系统中虚拟密码机数量

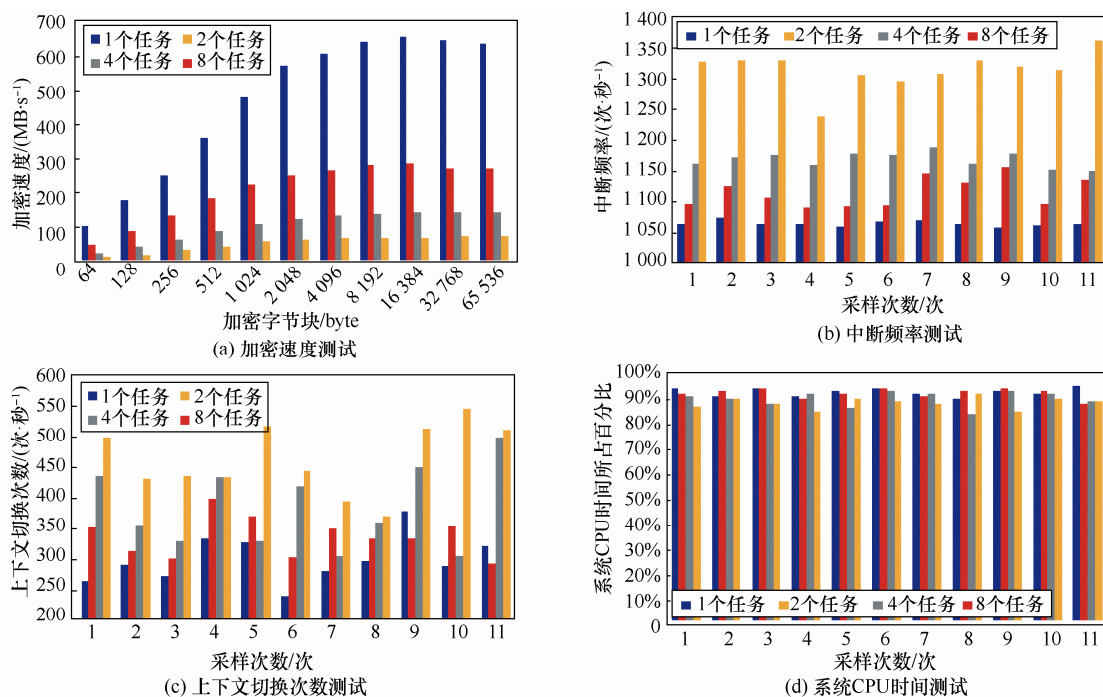


图7 单台虚拟密码机性能测试

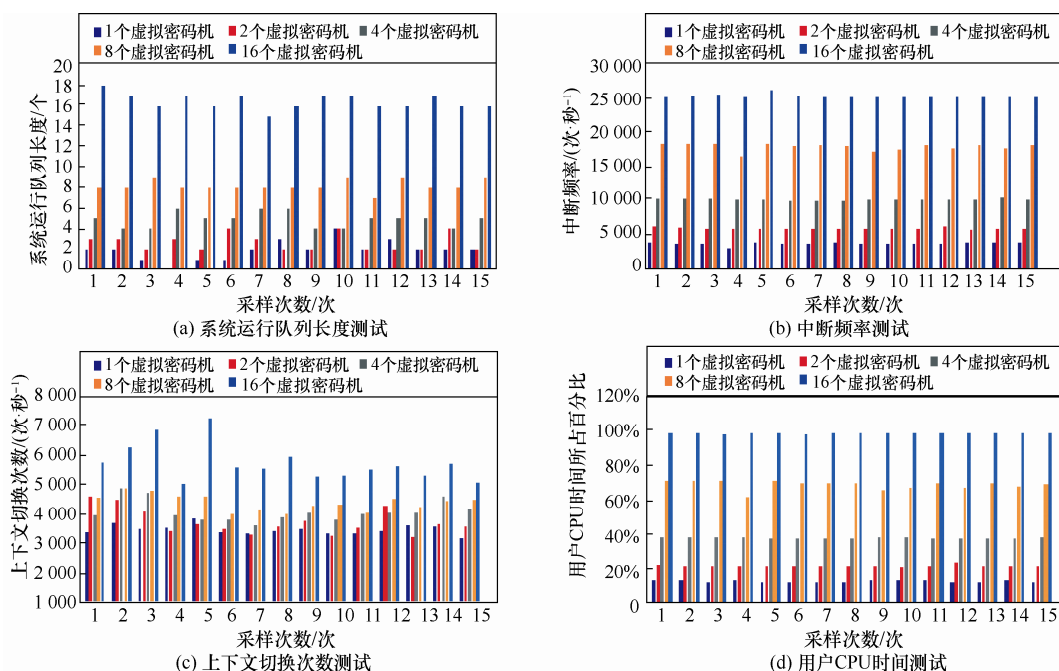


图 8 多台虚拟密码机性能测试

增加时, 系统运行队列长度和系统中断频率明显增大, 且当系统运行 16 台虚拟密码机时, 系统运行队列长度与系统中断频率的比值明显增大, 该比值即为中断请求的排队等待时间, 该结果验证了中断频率过大使中断排队时间变长的结论。图 8(c)和图 8(d)所示, 系统的上下文切换次数随虚拟密码机数量的增加而增加, 用户 CPU 时间也随虚拟密码机数量的增加而急剧增加。当运行 16 台虚拟密码机时, 用户 CPU 时间达到 100%, 说明系统加解密频繁, CPU 繁忙。

综合上述测试结果, 不管单台虚拟密码机还是多台虚拟密码机, 密码运算任务越多, 系统中断频率和系统上下文切换次数越多, 更多的 CPU 资源则用来处理系统调用, 致使系统 I/O 繁忙, 密码任务的请求响应时间变长, 进而影响密码运算的速度, 导致加密字节达到一定值时密码运算速度呈现降低的趋势。要提高虚拟密码机密码运算速率, 就要保证 I/O 传输的高效性, 控制系统中断频率和系统上下文切换次数可有效提高 I/O 传输能力, 因此, 影响 SR-IOV

密码设备系统性能的关键因素是中断频率和上下文切换次数。

5 结束语

本文从 SR-IOV 密码设备相关技术入手, 分析了中断是一种有效满足密码任务实时性要求的通信机制, 然而也带来了严重的开销问题。首先, 虚拟环境下的中断传输机制相比物理环境下更复杂, 中断请求在传输过程中被 VMM 两次截获, 造成严重的上下文切换, 增大了系统开销; 其次, 当虚拟环境下中断请求频率过高时, 会严重降低 SR-IOV 密码设备处理密码运算的能力。本文针对 SR-IOV 密码设备处理密码任务的特点建立了 M/M/1 排队模型, 分析了影响 SR-IOV 密码设备密码运算性能的因素, 通过仿真和实验两种方式, 对系统队列长度、系统中断频率、系统上下文切换次数、系统 CPU 时间和用户 CPU 时间进行了测试和分析, 并对模型的有效性进行了验证。结果表明, 本文建立的模型对 SR-IOV 密码设备中断传输过程的分析具有较高的有效性。

本文关于 SR-IOV 密码设备中断传输过程模型的建立仅适用于某一类密码服务的情况, 后续的研究将拓展到密码云环境, 对密码云环境下不同类和不同优先级的密码服务进行建模, 研究影响 SR-IOV 密码设备密码运算性能的各项因素。

参考文献:

- [1] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. An overview of cloud computing environment security[J]. Journal of Software, 2016, 27(6): 1328-1348.
- [2] 郭松辉, 李清宝, 孙磊, 等. 基于 ISSM 的密码服务系统虚拟化性能建模[J]. 系统仿真学报, 2017, 29(8):1692-1701.
GUO S H, LI Q B, SUN L, et al. Performance modeling of cryptographic service system virtualization based on ISSM[J]. Journal of System Simulation, 2017, 29(8):1692-1701.
- [3] 牛欣源. 实时任务模型中的性能解析——中断性能研究[J]. 计算机科学与技术, 2014(2):55-64.
NIU X Y. Real-time task model performance analysis——interrupt performance research[J]. Transactions on Computer Science and Technology, 2014(2):55-64.
- [4] 王泽武, 孙磊, 郭松辉. 基于滚动优化的密码云实时任务阈值调度方法[J]. 计算机应用, 2017, 37(10):2780-2786.
WANG Z W, SUN L, GUO S H. Real-time task threshold scheduling method by rolling optimization in cryptography cloud[J]. Journal of Computer Application, 2017, 37(10):2780-2786.
- [5] DONG Y, YANG X, LI J, et al. High performance network virtualization with SR-IOV[J]. Journal of Parallel and Distributed Computing, 2012, 72(11):1471-1480.
- [6] XU X, DAVDA B. A hypervisor approach to enable live migration with pass through sr-iov network devices[J]. Acm Sigops Operating Systems Review, 2017, 51(1): 15-23.
- [7] YOUNGE A J, WALTERS J P, CRAGO S P, et al. Supporting high performance molecular dynamics in virtualized clusters using IOMMU, SR-IOV, and GPUDirect[C]//ACM Sigplan/Sigops International Conference on Virtual Execution Environments. 2015:31-38.
- [8] 李帅, 孙磊, 郭松辉. 减少上下文切换的虚拟密码设备中断路径优化方法[J]. 计算机应用, 2018, 38(7):1946-1950.
LI S, SUN L, GUO S H. A method to reduce interrupt path of virtual cryptographic device with context switching[J]. Journal of Computer Application, 2018, 38(7):1946-1950.
- [9] DONG Y, YANG X, LI X, et al. High performance network virtualization with SR-IOV[C]// IEEE International Symposium on High Performance Computer Architecture. 2010:1471-1480.
- [10] DONG Y, XU D, ZHANG Y, et al. Optimizing network I/O virtualization with efficient interrupt coalescing and virtual receive side scaling[C]//IEEE International Conference on Cluster Computing. 2011:26-34.
- [11] GUAN H B, DONG Y Z, TIAN K, et al. SR-IOV based network interrupt-free virtualization with event based polling[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(12): 2596-2609.
- [12] LI J, XUE S, ZHANG W, et al. When I/O interrupt becomes system bottleneck: efficiency and scalability enhancement for SR-IOV network virtualization[J]. IEEE Transactions on Cloud Computing, 2017, PP(99): 1-1.
- [13] GORDON A, AMIT N, HAR'EL N, et al. ELI: bare-metal performance for I/O virtualization[C]//The 17th International Conference on Architectural Support for Programming Languages Operating Systems. 2012:411-422.
- [14] TU C C, FERDMAN M, LEE C T, et al. A comprehensive implementation and evaluation of direct interrupt delivery[C]//ACM Sigplan/Sigops International Conference on Virtual Execution Environments. 2015:1-15.
- [15] 王泽武. 密码服务云管理与调度技术研究[D]. 郑州: 战略支援部队信息工程大学, 2018.
WANG Z W. Research on management and scheduling technique of cryptographic service cloud[D]. Zhengzhou: Strategic Support Force Information Engineering University, 2018.
- [16] 米翔. 高性能网络虚拟化下的适应性中断调度和系统[D]. 上海: 上海交通大学, 2013.
MI X. Adaptive interrupt-free system in high performance I/O virtualization[D]. Shanghai: Shanghai Jiaotong University, 2013.
- [17] 唐加山. 排队论及其应用[M]. 北京: 科学出版社, 2016.
TANG J S. Queuing theory and its application[M]. Beijing: Science Press, 2016.
- [18] DUTTA Y, SETHI V. Performance analysis of cryptographic acceleration in multicore environment[M]//Quality, Reliability, Security and Robustness in Heterogeneous Networks. Springer, 2013.

[作者简介]



孙磊(1973—), 男, 江苏靖江人, 博士, 信息工程大学教授, 主要研究方向为网络空间安全、可信计算。



李帅(1994—), 男, 河南驻马店人, 信息工程大学硕士生, 主要研究方向为云计算安全、I/O 虚拟化性能优化。



郭松辉(1979—), 男, 四川乐山人, 博士, 信息工程大学副教授, 主要研究方向为云计算安全。