ISM:漂移意图可感知的 IP 网络生存性服务提供模型

赵二虎[1,2],阳小龙[1,3],徐 杰[1],隆克平[1,3],张 丹[4]
(1.电子科技大学通信与信息工程学院光互联网及移动信息网络研究中心,四川成都 611731;
2.中国科学院软件研究所综合信息系统技术国家级重点实验室,北京 100190;
3.北京科技大学计算机与通信工程学院,北京 100083; 4.中国航天二院七〇六研究所,北京 100854)

摘 要: 由于传统的服务漂移方法存在一定不足,致使服务器集群的负担较重,且服务漂移的时间开销过大,严重影响服务连续性.为了改善这种情况,本文提出了一种漂移意图可感知的 IP 网络生存性服务提供模型(Intent-perceived Service Migration,ISM).在 ISM 模型中,我们设计了一种独特的服务漂移触发机制和目标节点选取策略,并通过服务器与客户端的协作,使客户端对服务器集群内部的服务漂移意图有了预感知能力.分析结果表明,ISM 模型既能在时间和空间上保证服务漂移的随机性,增强服务抗毁度;又能显著减小由服务漂移带来的服务间断时间,有效提高了 IP 网络服务可生存性.

关键词: IP 网络生存性; 服务漂移; 伪随机序列; 抗毁度; 间断时间
中图分类号: TP393.02 **文献标识码:** A **文章编号:** 0372-2112 (2011) 12-2768-08

ISM: Intent-Perceptible Service Migration Model for IP Network Survivability

ZHAO Er-hu[1,2], YANG Xiao-long[1,3], XU Jie[1], LONG Ke-ping[1,3], ZHANG Dan[4]
(1. *Research Centre for Optical Internet and Mobile Information Networks, University of Electronic Science and Technology of China, Chengdu, Sichuan* 611731, *China*;
2. *National Key Lab of Integrated Information System Tech, Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*;
3. *School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing* 100083, *China*;
4. 706 *Institute, The Second Academy of China Aerospace, Beijing* 100854, *China*)

Abstract: The existing service migration methods bring the server cluster heavy burden, and their time spending is so high that seriously affects the service continuity. In order to enhance the survivability of IP network services, the paper puts forward an intent-perceptible service migration model (ISM). In this model, we design a novel trigger mechanism and object selecting method for service migration, and make the service migration intention perceptible for the client with the cooperation of the server. The evaluation results show that ISM model can not only ensure the service invulnerability by maintaining a high randomness of service migration, but also improve the service continuity by reducing the service gap time spending on service migration to the maximum extent. Therefore, ISM model can enhance IP network survivability efficiently.

Key words: IP network survivability; service migration; pseudo-random sequence; invulnerability; gap time

1 引言

网络生存性主要是指网络在遇到外部攻击或自身故障等突发异常情况下,仍能继续提供信息服务的能力[1,2].目前,国内外已开始对 IP 网络生存性的通用机理和调控方法展开深入系统的研究,研究角度主要包括类生态学[3,4]、拓扑抗毁[5,6]、容错容侵[7~9]、异常检测[10~12]、服务漂移[13,14,15~26]等.其中,服务漂移是指系统主动或被动地将服务从当前节点迁移到另一工作状况良好的节点上继续提供服务的技术.它可以通过采用负载分担、数据备份、服务恢复、服务重启等方法,在网络负载过重或遭受生存威胁等情况下,最大限度地保证服务连续性,因而具有重要的研究价值.

现有的服务漂移策略主要在服务器集群内部来实现.如文献[13,14]提出在服务器集群中采用随机自治可生存调度算法(SASS)来实施服务漂移.服务器在开

收稿日期:2011-01-11;修回日期:2011-05-16
基金项目:国家 973 计划课题(No.2007CB310706);国家自然科学基金项目(No.60725104, No.60873263, No.60932005);国家 863 计划课题(No.2009AA01Z215);四川省青年基金项目(No.09ZQ026-032);教育部新世纪优秀人才计划

始提供服务的同时,启动内部的伪随机序列产生器,一旦随机序列输出为'1',就停止当前服务器,其余备份服务器通过自由竞争机制来接替当前服务器继续提供服务.与 DNS 动态解析[15,16]、HTTP 报文重定向[17,18]、IP 报文重定向[19]等传统方法相比,SASS 方法不需要前端调度器,消除了前端节点所存在的安全瓶颈,同时有效保证了服务漂移在目标节点选取方面的随机性,但该方法也明显地存在以下三个方面不足:(1)由于在随机序列输出为'0'时不会触发服务漂移,那么在较长的'0'游程期间攻击者就可能有充足的时间来攻破当前服务器;(2)备份服务器之间的自由竞争机制会占用大量网络带宽和处理时间,增加了服务器集群的负担;(3)服务漂移的触发机制略显死板且漫无目的,漂移频率过快导致服务间断时间较大,势必对实时性要求较高的业务造成影响.文献[21]对文献[14]中的服务漂移触发机制做了改进,提出了"循环触发"的概念,即每隔特定时间就产生一个时隙作为服务漂移触发点,如果时隙在'0'游程期间到达,同样可以触发服务漂移.同时文献[21]引入了令牌机制,让负载最低的备份服务器优先获得令牌,一旦服务漂移触发,持有令牌的备份服务器就接替主服务器提供后续服务.与自由竞争机制相比,令牌机制可以减少目标节点的选取时间,但令牌机制存在固有的缺陷:如果某备份服务器长期处于低负载状态,那么它获持令牌的概率就高,从而使目标节点选取的随机性降低.文献[22]在文献[14]的基础上增加了入侵检测系统,当检测到外部攻击时就主动实施服务漂移,有效提高了服务漂移的主动性,但仍缺乏对自身健康状况的监测,而健康状况会直接影响到服务可生存性.此外,以上文献都是仅从服务器的角度来考虑服务漂移,主要体现在集群内部的进程迁移上,而客户端则一直处于接收服务的状态,没有参与服务漂移的实施.如果客户端能提前感知到服务器集群内部的服务漂移意向,那么在主服务器向备份服务器迁移服务的同时,客户端就可以尝试与备份服务器建立连接,减小服务漂移时耗.

基于以上考虑,本文提出了一种漂移意图可感知的 IP 网络生存性服务提供模型(Intent-perceptible Service Migration,ISM).该模型不仅在时间和空间上保证了服务漂移的随机性,提高服务抗毁度;而且实现了客户端对服务器集群内部服务漂移意图的预感知功能,可以大幅缩减由服务漂移带来的服务间断时间,从而在减少系统开销与提高服务可生存性之间取得最佳平衡.

2　问题描述

考虑这样一个网络场景:IP 网络上一用户向远程可用服务器请求 HTTP 服务.客户端用 Client 表示,服务器集群表示为 $S=\{S_1,S_2,S_3,\cdots\}$,假设 S_1、S_2、S_3 的功能相同或相似,且互为备份服务器.当 S_1 向 Client 提供服务时,如果出现外部网络攻击或者 S_1 自身健康状况恶化,都可能导致服务中断,所以在这种情况下是最应当触发服务漂移的;另一方面,当未出现任何异常时,也可以考虑让服务在集群内主动漂移以增加服务抗毁能力.因此如何设计一种合理的服务漂移触发机制,是其关键问题之一.

服务漂移触发之后,涉及到一个目标节点选取的问题.如果按照特定的顺序来选择目标节点,比如 $S_1\rightarrow S_2\rightarrow S_3\rightarrow S_1$,则会有较大的安全隐患,因为固定的服务漂移顺序易被攻击者掌握,成为其实施攻击的有力工具,从而使服务漂移失去了应有的效果.为确保服务漂移的有效性,必须保证服务漂移意图在攻击者看来是行踪不定的,以使攻击者无法准确找到攻击目标.因此如何建立一种高度随机的服务漂移模式,是其关键问题之二.

已有的服务漂移策略[13,14]大多采用"先漂移后连接"的方法,即先将主服务器上的服务迁移到备份服务器上,然后备份服务器再与客户端之间建立连接.这种方法使服务漂移的全部工作量都由服务器承担,造成服务器集群的负担较重;且服务漂移过程的时耗较大,致使服务间断时间较长.因此如何降低服务漂移的时耗,从而最大程度上减小由服务漂移所带来的服务间断时间,是其关键问题之三.

3　ISM 模型与算法实现

在具体描述 ISM 模型之前,先做以下假设:

假设 1　服务漂移主要针对图 1 所示的 IP 端到端服务(Client-Server 模式),其中客户端(Client)和服务器集群(Server Cluster)分别通过边界路由器 IP Router *a* 和 IP Router *b* 连接到 IP 网络中.

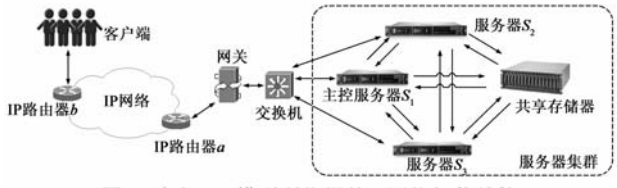


图1　建立ISM模型所依据的IP网络拓扑结构

假设 2　集群内的服务器(S_1,S_2,S_3)互为备份服务器,可以向 Client 提供相同或相似的服务,且它们之间能够互通信息,这些信息包括工作日志、服务状态、健康状况等.

假设 3　Client 和 Server Cluster 两端的接入网不会发生灾难性故障,尤其是边界路由器要工作稳定,使 Client 与 Server Cluster 之间可以随时建立连接,这是保证服务漂移具有可行性的前提.

假设 4 以下对 ISM 模型的论述均是在假设 Client 已被排除是恶意节点的情况下完成.

3.1 ISM 模型的服务漂移触发机制

ISM 模型从三个方面来考虑服务漂移的触发问题,分别是遭受外部攻击、自身健康状况恶化和正常状态下的主动服务漂移,并建立了异常事件触发与伪随机序列触发相结合的触发机制.

我们把外部攻击对服务器的威胁程度(用 L 表示)由弱到强进行分级,如 $L_0, L_1, L_2, \cdots, L_{\text{top}}$;把服务器集群的网关防护级别(用 D 表示)由低到高进行分级,如 $D_0, D_1, D_2, \cdots, D_{\text{top}}$. 当服务器遭受到外部攻击时,先评估当前攻击的威胁程度,然后根据网关防护级别来决定是否触发服务漂移. 假如威胁程度在网关的防护级别之内,即 $L < D$,则不影响服务器正常工作,不触发服务漂移;如果攻击的威胁程度超过了网关的防护级别,即 $L \geqslant D$,有可能会导致服务中断,遂触发服务漂移.

由于服务器自身健康状况也会影响服务的可生存性,所以我们把服务器健康状况纳入到了服务漂移的触发因素之列,并将服务器的健康指数(用 H 表示)由弱到强分为不同等级,如 $H_0, H_1, H_2, \cdots, H_{\text{top}}$,同时设置服务漂移阈值(用 $H_{\text{threshold}}$表示). 在服务器对外提供服务期间,我们选择负载最低的备份服务器来监测当前服务器的健康状况,并计算其健康指数. 如果 $H > H_{\text{threshold}}$,表示当前服务器的运行环境比较安全;如果 $H \leqslant H_{\text{threshold}}$,表明当前服务器的健康状况恶化,应及时将服务迁移到备份服务器上,并把当前服务器转入修复状态.

综合上述两个方面,我们建立了服务漂移的异常事件触发机制,并用变量 V_{abnormal}作为服务漂移触发信号,其定义式如下:

$$V_{\text{abnormal}} = \begin{cases} \left(1 - \dfrac{\min((D-L),(H-H_{\text{threshold}}))}{|\min((D-L),(H-H_{\text{threshold}}))|}\right) \div 2, & D \neq L \text{ 且 } H \neq H_{\text{threshold}} \\ 1, & D = L \text{ 或 } H = H_{\text{threshold}} \end{cases} \tag{1}$$

由式(1)可知,V_{abnormal}的取值为 1 或 0. 当 $V_{\text{abnormal}} = 1$ 时,触发服务漂移;当 $V_{\text{abnormal}} = 0$ 时,则维持当前服务器的服务状态. 这种异常事件触发机制可以在外部攻击或自身健康状况恶化等异常情况下触发服务漂移,确保了服务漂移的合理性.

下面考虑正常状况下主动实施服务漂移的情况. 我们在服务器集群内部建立了一种伪随机序列触发机制,并把伪随机序列的上升沿(即从'0'电平到'1'电平的跳变)作为服务漂移的触发信号(用 b_{nor}表示),具体可以通过下式来计算:

$$b_{\text{nor}}(k) = \overline{\overline{b_k + b_k} + b_{k-1}} \tag{2}$$

其中 b_k 和 b_{k-1}是序列的两个相邻比特位,只有当出现上升沿(即 $b_{k-1} = 0$ 且 $b_k = 1$)时 b_{nor}才等于 1,其余情况下 b_{nor}都等于 0. 如果 $b_{\text{nor}} = 1$,即触发服务漂移;如果 $b_{\text{nor}} = 0$,则当前服务器继续提供服务. 由伪随机序列的性质[27]可知,这种伪随机序列触发机制能确保服务漂移在触发时间上的随机性.

ISM 模型结合了以上两种触发机制,并用变量 S_{tri} 作为服务漂移的总触发信号,其定义式如下:

$$S_{\text{tri}} = V_{\text{abnormal}} \| b_{\text{nor}} \tag{3}$$

其中运算符 ‖ 表示逻辑或运算. 在 ISM 模型中,我们设定在 $S_{\text{tri}} = 1$ 时触发服务漂移,在 $S_{\text{tri}} = 0$ 时则维持当前服务. 由式(3)可知,在 V_{abnormal}与 b_{nor}两者之间任何一个变量为 1 的情况下 ISM 模型均会触发服务漂移,因而确保了服务漂移在触发时间上的合理性与随机性.

3.2 ISM 模型的目标节点选取方法

在目标节点选取方面,我们设计了一种基于游程长度的目标节点选取方法,即根据服务漂移触发时刻的前一时刻所记录的游程长度来计算目标节点. 设集群内服务器个数为 n,服务漂移触发时刻为 k,且触发的前一时刻所记录的游程长度为 r_{k-1},那么服务漂移的目标节点(用 o_k 表示)可以通过下式来计算:

$$o_k = (r_{k-1} \bmod n) + 1 \tag{4}$$

其中,mod 表示模运算. 例如,当 $r_{k-1} = 10$, $n = 3$ 的时候得出 $o_k = 2$,表示在 k 时刻触发服务漂移,目标节点为服务器 S_2;如果当前服务器即为 S_2,则表示让 S_2 继续提供服务. 根据伪随机序列的性质[27]可知,伪随机序列中的游程长度是随机出现的且具有一定的统计特性,这就保证了服务漂移的目标节点选取在空间上是随机性. 表 1 给出了服务器集群在一个伪随机序列 b_k 作用下的服务漂移情况,其中 $n = 3$ 表示集群内有三个服务器(S_1、S_2、S_3). 先由式(2)计算出触发信号 b_{nor}的值,可以得出服务漂移的触发时刻依次为 $k = 9$、16、19,然后根据触发前一时刻所记录的游程长度(即 $r_8 = 6$、$r_{15} = 2$、$r_{18} = 1$),通过式(4)可以计算出三次服务漂移的目标节点依次为 $o_9 = S_1$、$o_{16} = S_3$、$o_{19} = S_2$.

3.3 ISM 模型的漂移意图感知机制

ISM 模型通过在服务器集群内构建线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)来产生伪随机序列(本文采用的是 m 序列),用以触发服务漂移和目标节点选取. 具体的伪随机序列理论可参考文献[27],这里不做重复性介绍. 图 2 给出了 ISM 模型所采用的 LFSR 的结构图,其反馈函数可以表示为

$$b_k = c_1 b_{k-1} + c_2 b_{k-2} + c_3 b_{k-3} + \cdots + c_{l-1} b_{k-l+1} + c_l b_{k-l} \tag{5}$$

表 1　ISM 模型在伪随机序列作用下的服务漂移触发与目标节点选取($n=3$)

时间(k)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	…
伪随机序列(b_k)	X	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	1	1	0	1	1	1	…
游程长度(r_k)	X	1	2	1	2	3	4	5	6	1	2	3	4	5	1	2	1	2	1	1	2	3	…
触发信号(b_{nor})		X	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0		…
目标节点(o_k)										1 (S_1)							3 (S_3)			2 (S_2)			…

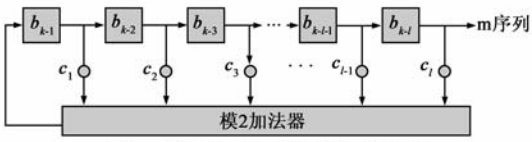


图2　l级线性反馈移位寄存器框图

对应的联接多项式可以表示为

$$f(x)=c_0+c_1x+c_2x^2+\cdots+c_lx^l,(c_0=c_l=1) \quad (6)$$

我们都知道,LFSR 的逻辑功能完全由反馈函数所标识,如果知道了 LFSR 的联接多项式 $f(x)$,便立即可以求得相应的反馈函数.此外,m 序列的生成过程还受初始向量和系统时钟两个因素影响.

由序列密码产生的原理[28]可知,在联接多项式为已知而初始向量为随机的情况下,所产生的 0-1 序列是难以预测的,于是针对同种类型的服务,所有服务器均采用相同的联接多项式和互异的非零初始向量来构建各自的 LFSR;针对不同类型的服务则选择不同的联接多项式.假设 Client 同时请求了 3 种类型的服务,分别为 a,b,c,用 S_{ty}来表示 Client 所请求服务的类型集合,则有:

$$\boldsymbol{S}_{ty}=\{a,b,c\} \quad (7)$$

与 $\boldsymbol{S}_{ty}$相对应的联接多项式集合可表示为

$$\boldsymbol{F}(\boldsymbol{S}_{ty})=\{f_a(x),f_b(x),f_c(x)\mid f_a(x)\neq f_b(x)\neq f_c(x)\} \quad (8)$$

其中 $f_a(x)$是指服务器集群在提供 a 类型服务时的 LFSR 联接多项式.服务器 S_1 上针对 S_{ty}的 LFSR 初始向量集合可表示为

$$\boldsymbol{P}_{S_1}(\boldsymbol{S}_{ty})=\{p_{S_1,a},p_{S_1,b},p_{S_1,c}\mid p_{S_1,a}\neq 0,p_{S_1,b}\neq 0,p_{S_1,c}\neq 0\} \quad (9)$$

其中 $p_{S_1,a}$是指服务器 S_1 在提供 a 类型服务时所选用的 LFSR 初始向量.那么针对服务类型集合 $\boldsymbol{S}_{ty}$,服务器集群内的所有初始向量可以用集合表示为:

$$\begin{aligned}\boldsymbol{P}&=\{\boldsymbol{p}_a,\boldsymbol{p}_b,\boldsymbol{p}_c\mid \boldsymbol{p}_a\neq 0,\boldsymbol{p}_b\neq 0,\boldsymbol{p}_c\neq 0\}\\&=\Big\{\{p_{a,S_1},p_{a,S_2},p_{a,S_3}\},\{p_{b,S_1},p_{b,S_2},p_{b,S_3}\},\\&\quad\{p_{c,S_1},p_{c,S_2},p_{c,S_3}\},\mid p_{a1}\neq p_{a2}\neq p_{a3}\neq 0,\\&\quad p_{b1}\neq p_{b2}\neq p_{b3}\neq 0,p_{c1}\neq p_{c2}\neq p_{c3}\neq 0\Big\}\end{aligned} \quad (10)$$

有了以上对 LFSR 组成因素的分析和提取,我们可以在客户端也建立同样的伪随机序列产生器,实现 Client 对集群内部服务漂移意图的感知功能.在 ISM 模型中,服务漂移将同时执行两个进程,一个是主服务器与备用服务器之间的服务状态迁移,另一个是备用服务器与客户端之间建立连接.假设集群中 S_1 第一个向 Client 提供服务,首先 S_1 会根据 Client 所请求的服务类别($\boldsymbol{S}_{ty}$)选择合适的联接多项式($\boldsymbol{F}$)和初始向量($\boldsymbol{p}_{S_1}$)来组建 LFSR(命名为 S_1-LFSR),然后向备份服务器广播 $\boldsymbol{F}$,同时把 $\boldsymbol{F}$ 和 $\boldsymbol{p}_{S_1}$发送给 Client.备份服务器在接收到 $\boldsymbol{F}$ 后,会随机选择初始向量来组建各自的 LFSR;Client 接收到 $\boldsymbol{F}$ 和 $\boldsymbol{p}_{S_1}$之后,也会立即组建运行在客户端的 LFSR(命名为 C-LFSR).上述过程完成之后,C-LFSR 与 S_1-LFSR 会依次启动,这样 Client 就可以掌握集群内 S_1 的服务漂移触发时间点和目标节点.一旦 Client 从 C-LFSR 所产生的 m 序列中计算出服务漂移的触发时刻和目标节点(假如是 S_3),那么在 S_1 向 S_3 迁移服务的同时,Client 就开始与 S_3 建立连接.如果 S_3 响应了 Client 的连接请求,它会首先将 S_3-LFSR 的初始向量 $\boldsymbol{p}_{S_3}$发给 Client,用以重建 C-LFSR.为形象说明漂移意图感知机制是如何实现的,图 3 给出了 Client 与服务器集群之间建立 TCP 连接的具体过程.

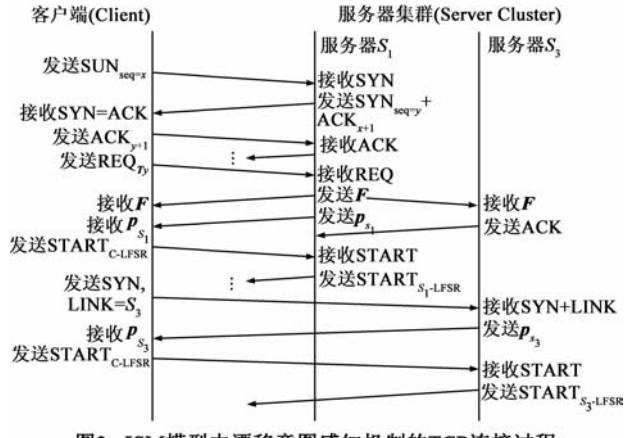


图3　ISM模型中漂移意图感知机制的TCP连接过程

3.4　ISM 模型的算法实现

ISM 模型的算法流程如图 4 所示,包括 5 个功能模块.

功能块 1:建立连接模块.假设 S_1 第一个响应 Client 的服务请求,首先组建 S_1-LFSR 和 C-LFSR.一旦 Client 完成 C-LFSR 的组建,即刻开启 C-LFSR,并向 S_1 发送启动信号.如果 S_1 在规定时间内接收到 C-LFSR 的启动信号,就转入功能块 2、3、4 执行,否则循环执行功能块 1;

功能块 2:健康监测模块.在备份服务器中选择负载

最低的服务器来监测 S_1 的健康状况.当计算出 S_1 的健康指数 H 后,将 H 与服务漂移阈值 $H_{\text{threshold}}$进行比较,以判断是否触发服务漂移.如满足服务漂移的触发条件,则转到功能块 5 继续执行,否则循环执行功能块 2;

功能块 3:入侵检测模块.启动 S_1 的入侵检测进程,监视外部网络攻击情况,并评估其威胁等级 L.将 L 与网关防护级别 D 作比较,如满足服务漂移触发条件,则转到功能块 5 执行,否则循环执行功能块 3;

功能块 4:伪随机序列生成模块.启动 S_1-LFSR 以产生 m 序列,并统计其游程长度.根据式(2)计算 b_{nor},判断其是否满足触发条件.若 $b_{\text{nor}}=1$,则转到功能块 5 执行服务漂移,否则循环执行功能块 3;

功能块 5:服务漂移执行模块.先根据式(4)计算服务漂移的目标节点(假设是 S_3),然后 S_1 压缩当前的服务状态信息并发送给 S_3.同时 Client 开始与 S_3 建立连接,并由 S_3 提供后续服务.服务漂移完成.

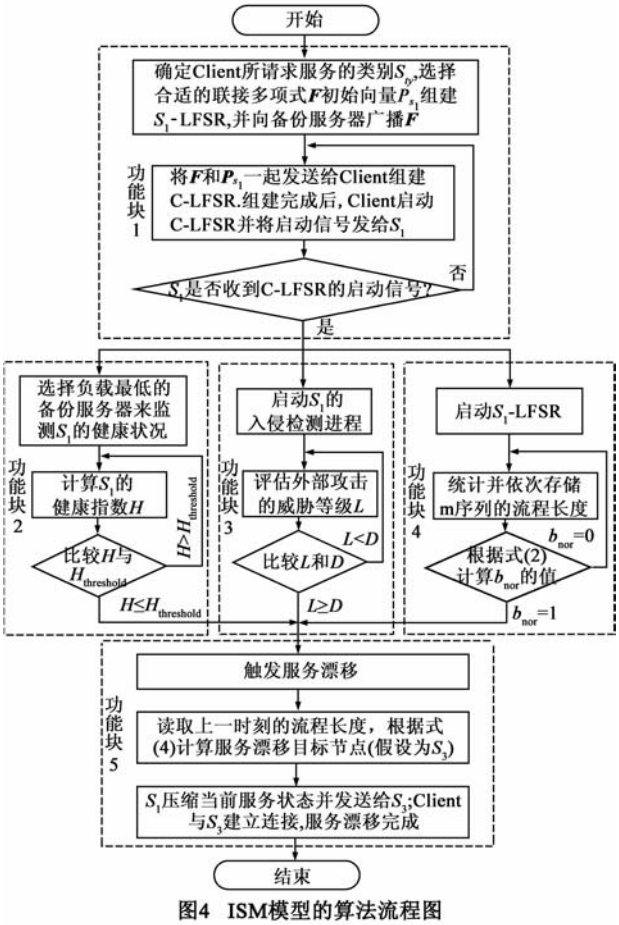


图4 ISM模型的算法流程图

4 性能分析与评估

本节将 ISM 模型与文献[14]的 SASS 模型以及文献[21]的 TOKEN 模型进行比较,主要从服务抗毁度和服务间断时间两个方面来评估它们的性能.下面先给出服务抗毁度的定义.

定义 1 服务抗毁度(用 R_d 表示):假设集群内的服务器个数为 n,服务漂移到第 i 个备份服务器的概率为 P_i,借鉴信息熵的概念,服务抗毁度可表示为

$$R_d=-\sum_{i=1}^{n}P_i\ln(P_i),\ n\geqslant 2 \tag{11}$$

R_d 值越大说明服务漂移的随机性越高,则攻击者捕获服务漂移信息的难度就越大,从而反映出服务的抗毁度越高.

在 SASS 模型中,随机序列输出'0'或'1'的概率均为 1/2,但只有'1'是服务漂移的触发信号,所以触发概率为 1/2.当发生服务漂移时,SASS 模型从 $n-1$ 个备份服务器中选择一个作为新主服务器;如果不发生服务漂移,则仍由当前服务器继续提供服务.假如各备份服务器竞争成为主服务器的概率相等,那么根据式(11)可得出 SASS 的服务抗毁度为

$$R_d=-\left[\frac{1}{2}\log\left(\frac{1}{2}\right)+(n-1)\frac{1}{2(n-1)}\log\left(\frac{1}{2(n-1)}\right)\right] \tag{12}$$

由式(12)可以计算出 SASS 模型在不同服务器个数下的服务抗毁度,如图 6 中 SASS 曲线所示,可见 SASS 模型的服务抗毁度是随着服务器个数的增加而增大的.

在 TOKEN 模型中,当服务漂移触发之后,会从 $n-1$ 个备份服务器中选择负载最低的服务器作为新主服务器,因此 TOKEN 模型的服务抗毁度为

$$R_d=-\left[\frac{1}{2}\log\left(\frac{1}{2}\right)+n_o\times\frac{1}{2n_o}\log\left(\frac{1}{2n_o}\right)\right],1\leqslant n_o\leqslant n-1 \tag{13}$$

式(13)中的 n_o 是指备份池中负载最低的服务器个数.由于 TOKEN 模型在服务器集群中采用了负载均衡技术,所以 n_o 值的大小受负载均衡技术的影响,而最理想的情况是 $n-1$ 个备份服务器的负载都相同,因此 n_o 最大可取 $n-1$,最小值为 1.图 5 给出了 TOKEN 模型在不同场景下的服务抗毁度,其中横坐标表示集群中的服务器个数,纵坐标是依据式(13)计算出的服务抗毁度,5 条曲线分别对应 n_o 的 5 种不同取值(代表不同网络场景).可以看出,当 n_o 固定时,集群中服务器个数越多则服务抗毁度越大;在服务器个数确定的情况下,服务抗毁度随 n_o 的增加而变大,由此可见负载均衡技术的优劣直接影响了 TOKEN 模型的服务抗毁度的大小.

ISM 模型是依靠伪随机序列的上升沿来触发服务漂移的,目标节点的选取决定于上升沿之前的'0'游程长度,因此服务抗毁度的计算与伪随机序列中游程长度的分布特性是密不可分的.表 2 给出了在服务器个数为 2 的情况下(即 $n=2$)ISM 模型的服务抗毁度的具体计算方法.从表 2 可以看出,服务器个数 n 和移位寄存器阶数 l 均影响 ISM 模型的服务抗毁度大小.

图 6 给出了 ISM 模型、SASS 模型和 TOKEN 模型的服务抗毁度变化曲线.通过比较可以看出,ISM 的服务抗毁度大体上随着 l 和 n 的增加而变大.当 $2 \leqslant n \leqslant 4$ 时,SASS 模型的抗毁度最大,ISM 模型可以通过调节 l 值来获得与 SASS 相同或相近的抗毁度,并且均大于 TOKEN 在对应 n 值下的抗毁度;当 $n \geqslant 4$ 时,ISM 模型的服务抗毁度曲线均低于 SASS 曲线和 TOKEN 模型的最佳曲线($n_o = n - 1$ 的情况).不过当 $n_o \neq n - 1$ 的时候,ISM 模型的抗毁度可能高于 TOKEN 模型,例如在 $n = 8$ 且 $n_o = n - 5$ 的情况下,如果 l 取值大于 6,则 ISM 模型的抗毁度就大于 TOKEN 模型;如果 l 取值为 4,ISM 模型的值就低于 TOKEN 模型.由此可见,当集群中服务器个数不大于 4 的时候,ISM 模型的服务抗毁度可与最优者(SASS 模型)持平.

服务间断时间也是我们评价服务漂移模型的重要指标,因为服务漂移在提高服务抗毁度的同时会在一定程度上造成服务的间断,这直接影响到服务的连续性.下面先给出服务间断时间的定义.

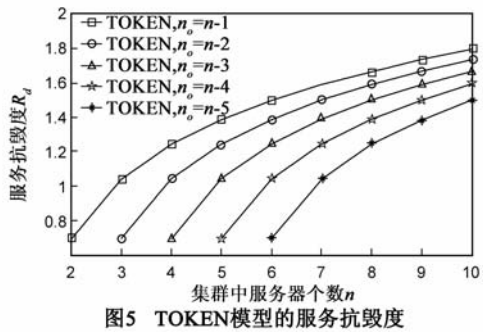


图5　TOKEN模型的服务抗毁度

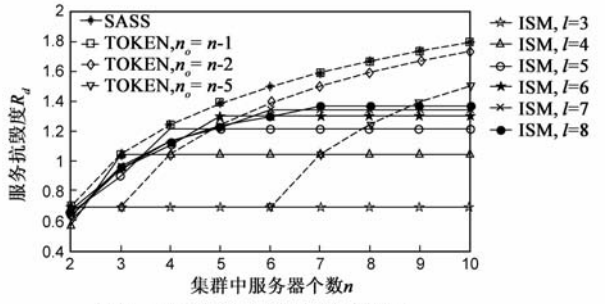


图6　三种模型的服务抗毁度对比

表 2　ISM 模型的服务抗毁度计算方法($n = 2$)

由 l 阶移位寄存器生成 m 序列,单周期内'0'游程总个数为 2^{l-2}									
'0'游程长度	1	2	3	4	5	6	…	$l-2$	$l-1$
在游程总个数中所占比例	1/2	1/4	1/8	1/16	1/32	1/64	…	$1/2^{l-2}$	$1/2^{l-2}$
对应的目标节点(S_1 或 S_2)	S_2	S_1	S_2	S_1	S_2	S_1	…	$S_{(l-2) \bmod 2+1}$	$S_{(l-1) \bmod 2+1}$
S_2 选取概率 $P(S_2)$	$1/2 + 1/8 + 1/32 + \cdots$								
S_1 选取概率 $P(S_1)$	$1/4 + 1/16 + 1/64 + \cdots$								
服务抗毁度 R_d	$-[P(S_2) \times \log P(S_2) + P(S_1) \times \log P(S_1)]$								

定义 2　服务间断时间(用 T_d 表示):假设服务器集群在完成一个服务过程中共发生了 M 次服务漂移,T_j 是第 j 次服务漂移所需的时间,则有

$$T_d = \sum_{j=1}^{M} T_j \tag{14}$$

由定义 2 可知,服务间断时间受服务漂移时间和服务漂移频率的影响.一般情况下服务漂移过程存在三个时间段:目标节点选取时间(用 T_{os} 表示)、主服务器向备用服务器迁移服务的时间(用 T_{sm} 表示)、以及备用服务器与客户端建立连接的时间(用 T_{ec} 表示).SASS 模型与 TOKEN 模型均采用"先漂移后连接"的方法,不同的是 SASS 模型通过自由竞争来选取目标节点,而 TOKEN 模型直接选取负载最低的备份服务器作为目标节点,节约了目标节点选取时间(用 T_{os} 表示),因此 SASS 模型执行一次服务漂移所需的时间为 $T_{os} + T_{sm} + T_{ec}$,而 TOKEN 模型执行一次服务漂移所需时间为 $T_{sm} + T_{ec}$.本文的 ISM 模型通过读取游程长度来计算目标节点,节省了目标节点选择时间,而且在服务迁移的同时即开始建立连接,因此 ISM 模型执行一次服务漂移所需的时间可以表示为 $T_{sm} + T_{ec} - T_x$,其中 T_x 是服务迁移与建立连接的重叠时间,且 $0 \leqslant T_x \leqslant \min(T_{sm}, T_{ec})$.图 7 形象地说明了 ISM 模型的单次服务漂移时间明显小于 SASS 模型和 TOKEN 模型.

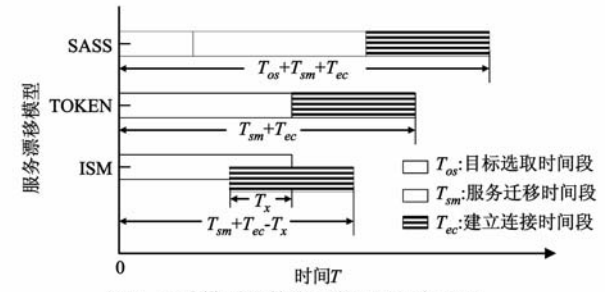


图7　三种模型的单次服务漂移时间对比

除单次服务漂移时间之外,漂移频率同样也影响着服务间断时间的大小.由于 ISM、SASS、TOKEN 三种模型都是基于伪随机序列来触发服务漂移的,因此我们可以考虑在伪随机序列的一个周期内的服务漂移次数(即单周期漂移次数).图 8 给出了在 m 序列作用下三种模型的单周期漂移次数.从图中可以看出,三种模型都是随着移位寄存器阶数 l 的变大呈指数增长趋势.由于 SASS 模型和 TOKEN 模型都是利用'1'信号来触发服

务漂移,而 ISM 模型利用随机序列中的上升沿来触发服务漂移,因此 ISM 模型的单周期服务漂移次数仅为 SASS 的一半.此外因 TOKEN 模型还增加了"循环触发"机制,所以它的实际单周期服务漂移次数会在 SASS 曲线的基础上有所升高,图 8 中的 a 表示在 m 序列单周期内出现的循环触发次数.由图 8 可知,ISM 模型的单周期服务漂移次数是最少的,再结合图 7 的分析,可以得出 ISM 模型因执行服务漂移所带来的服务间断时间显著小于 SASS 模型和 TOKEN 模型,证明了 ISM 模型既能提高服务抗毁度又能在一定程度上保持服务连续性.

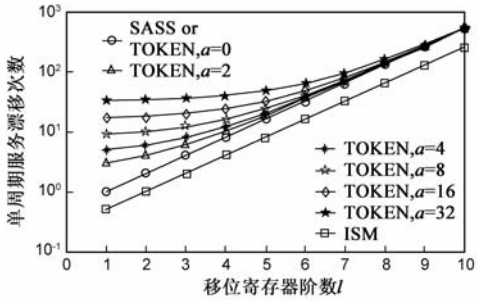


图8 在m序列单周期内的服务漂移次数

5 结论

本文讨论了一种用于提高 IP 网络服务可生存性的新型服务漂移模型.由于传统的服务漂移方法存在一定不足,致使服务器集群的负担较重,且服务漂移的时间开销过大,严重影响服务连续性.为了改善这种情况,从而保证 IP 网络服务的连续性,本文提出了一种漂移意图可感知的 IP 网络生存性服务提供模型(ISM).在 ISM 模型中,我们设计了一种独特的服务漂移触发机制和目标节点选取策略,并通过服务器与客户端的协作,使客户端对服务器集群内部的服务漂移意图有了预感知能力.

通过对 ISM 模型进行分析评估,并与 SASS 模型和 TOKEN 模型相比较,证明了 ISM 模型具有一定的优势:它既能保证服务漂移在触发时间上的随机性,也能在空间上满足目标节点的选取是行踪不定的,并可以在提高服务抗毁度的同时,显著减小服务间断时间,有效提高了服务连续性,对 IP 网络的生存性研究有一定启发意义.

致谢 感谢中国科学院软件研究所综合信息系统技术国家级重点实验室何晓新研究员给予的指导和帮助.

参考文献

[1] Ellison R J, Fisher D A, Linger R C, et al. Survivable Network Systems: An Emerging Discipline[R]. Pittsburgh, PA, US: Software Engineering Institute, Carnegie Mellon University, 1997.

[2] Knight J C, Sullivan K J. On the Definition of Survivability [R]. Charlottesville, VA, US: Dept of Computer Science, University of Virginia, 2000.

[3] Suda T, Nakano T, Moore M, Enomoto A, Fujii K. Biologically inspired approaches to networks: The bio-networking architecture and the molecular communication[A]. Proc of the Bio-Inspired Computing and Communication, First Workshop on Bio-Inspired Design of Networks (BIOWIRE'07)[C]. Berlin Heidelberg, Germany: Springer-Verlag Press, 2008. 241 – 254.

[4] Wang M, Suda T. The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications[A]. Proc of 2001 Symposium on Applications and the Internet (SAINT'01)[C]. Washington, DC, US: IEEE Computer Society Press, 2001. 43 – 53.

[5] Weichenberg G, Chan V W S, Medard M. High-reliability topological architectures for networks under stress[J]. IEEE Journal on Selected Areas in Communications, 2004, 22(9): 1830 – 1845.

[6] 陈福,杨家海,杨扬.网络拓扑发现新算法及其实现[J].电子学报,2008,36(8):1620 – 1625.
CHEN Fu, YANG Jia-hai, YANG Yang. New algorithms on IP network topology discovery and its implement[J]. Acta Electronica Sinica, 2008, 36(8): 1620 – 1625. (in Chinese)

[7] Castro M, Liskov B. Practical Byzantine fault-tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398 – 461.

[8] LIAO Jianxin, ZHANG Cheng, LI Tonghong, ZHU Xiaomin. A quasi-optimal probabilistic fault localization algorithm in communication networks[J]. Chinese Journal of Electronics, 2011, 20(1): 151 – 154.

[9] Veríssimo P E, Neves N F, Correia M P. Intrusion-tolerant architectures: concepts and design[J]. Architecting Dependable Systems, 2003, LNCS 2677: 3 – 36.

[10] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey[J]. ACM Computing Surveys, 2009, 41(3): 15.1 – 15.58.

[11] 郑吉平,秦小麟,管致锦,孙瑾.可生存性 MLS/DBMS 中基于隐蔽通道的恶意事务检测[J].电子学报,2009,37(6):1264 – 1269.
ZHENG Ji-ping, QIN Xiao-lin, GUAN Zhi-jin, SUN Jin. Covert channel based malicious transaction detection in survivable MLS/ DBMS[J]. Acta Electronica Sinica, 2009, 37(6): 1264 – 1269. (in Chinese)

[12] Thottan M, Ji C Y. Anomaly detection in IP networks[J]. IEEE Transactions on Signal Processing, 2003, 51(8): 2191 – 2204.

[13] Huang Z G. The tenure duty method (TDM) in the active incident recovery research[A]. Proc of 5th International Workshop on Advanced Parallel Processing Technologies (APPT'

03)[C]. Berlin Heidelberg, Germany: Springer-Verlag Press, 2003.557 – 564.

[14] 黄遵国,卢锡城.随机自治可生存调度算法研究[J].计算机工程与科学,2005,27(3):1 – 3.
HUANG Zun-guo, LU Xi-cheng. On the algorithm for stochastic autonomous scheduling survivability[J]. Computer Engineering & Science, 2005, 27(3): 1 – 3. (in Chinese)

[15] Moon J B, Kim M H. Dynamic load balancing method based on DNS for distributed web systems[A]. Proc of the 8th International Conference on Electronic Commerce and Web Technologies (EC-Web'05)[C]. Berlin Heidelberg, Germany: Springer-Verlag Press, 2005.238 – 247.

[16] RFC 1794, DNS Support for Load Balancing[S]. IETF Working Group, 1995.

[17] Aparicio A C, Pascual J D. Load balancing in mobile IPv6's correspondent networks with mobility agents[A]. Proc of IEEE International Conference on Communications 2007 (ICC'07)[C]. New York, NY, US: IEEE Communications Society Press, 2007.1827 – 1832.

[18] RFC 1945, Hypertext Transfer Protocol-HTTP/1.0[S]. IETF Working Group, 1996.

[19] Gupta S, Narasimha Reddy A L. A client oriented IP level redirection mechanism[A]. Proc of the 18th Annual IEEE International Conference on Computer Communications (INFOCOM'99)[C]. New York, NY, US: IEEE Communications Society Press, 1999.1461 – 1469.

[20] Imai N, Isomura M, Horiuchi H. Flexible and seamless service migration for real-time communication with ubiquitous and heterogeneous networked resources[A]. Proc of the 47th Global Telecommunications Conference (GLOBECOM'04)[C]. New York, NY, US: IEEE Communications Society Press, 2004.988 – 994.

[21] 洪小亮,郭义喜.服务漂移机制的研究[J].信息工程大学学报,2008,9(1):105 – 109.
HONG Xiao-liang, GUO Yi-xi. Research on the mechanism of service migration[J]. Journal of Information Engineering University, 2008, 9(1): 105 – 109. (in Chinese)

[22] 张民贵,刘斌.IP 网络的快速故障恢复[J].电子学报,2008,36(8):1595 – 1602.
ZHANG Min-gui, LIU Bin. Fast failure recovery of IP networks[J]. Acta Electronica Sinica, 2008, 36(8): 1595 – 1602. (in Chinese)

[23] FU S, XU C. Service migration in distributed virtual machines for adaptive grid computing[A]. Proc of 2005 International Conference on Parallel Processing (ICPP'05)[C]. Washington, DC, US: IEEE Computer Society Press, 2005.358 – 365.

[24] 赵二虎,阳小龙,彭云峰,隆克平.CPSM:一种增强 IP 网络生存性的客户端主动服务漂移模型[J].电子学报,2010,38(9):2134 – 2139.
ZHAO Er-hu, YANG Xiao-long, PENG Yun-feng, LONG Ke-ping. CPSM: Client-side proactive service migration model for enhancing IP network survivability[J]. Acta Electronica Sinica, 2010, 38(9): 2134 – 2139. (in Chinese)

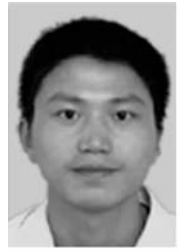
[25] Meeheam J, Livny M. A service migration case study: migrating the condor schedd[A]. Proc of Midwest Instruction and Computing Symposium (MICS'05)[C]. Red Hook, NY, US: Currant Associates, Inc, 2005.1 – 15.

[26] HAN Laiquan, WANG Jinkuan, WANG Xingwei. A function migration algorithm based on programmable router of multipath networks[J]. Chinese Journal of Electronics, 2011, 20(1): 170 – 174.

[27] 肖国镇,梁传甲,王育民.伪随机序列及其应用[M].北京:国防工业出版社,1985.
XIAO Guo-zhen, LIANG Chuan-jia, WANG Yu-min. Pseudo-random Sequence and Its Applications[M]. Beijing: National Defense Industry Press, 1985. (in Chinese)

[28] Rueppel R A. Analysis and Design of Stream Ciphers[M]. Berlin Heidelberg: Springer-Verlag Press, 1986.

作者简介



赵二虎　男,1985 年出生于河北邢台.中国科学院软件研究所工程师,主要从事软件无线电与认知无线网络方面的研究与开发.曾在电子科技大学通信与信息工程学院光互联网及移动信息网络研究中心从事 IP 网络生存性、移动自组网、无线通信等方面的研究.
E-mail: erhu@iscas.ac.cn

阳小龙　男,1970 年出生于四川广安.电子科技大学光互联网及移动信息网络研究中心教授、博士生导师,主要研究方向为光互联网体系结构、宽带网络理论与技术.
E-mail: yxl@uestc.edu.cn

徐　杰　男,1981 年生于四川成都,博士,电子科技大学讲师,主要研究方向为网络与信息安全理论与技术、混沌密码及保密通信技术.　E-mail: xuj@uestc.edu.cn

隆克平　男,1968 年生于四川通江,博士,北京科技大学计算机与通信工程学院院长,电子科技大学光互联网及移动信息网络研究中心主任,长江学者特聘教授、博士生导师,主要研究方向为高可信互联网理论与技术、光互联网体系结构和关键技术、宽带无线接入技术、电信增值业务等.　E-mail: lkp@uestc.edu.cn

张　丹　女,1984 年生于湖南汝城,中国航天二院七〇六研究所工程师,主要研究方向为物联网、无线通信与射频识别技术等.
E-mail: zhangdan_706@163.com