一种高效可扩展的自组织邻域故障检测协议

常光辉[①]　陈蜀宇[②]　徐光侠[①③]　卢华玮[①]
[①](重庆大学计算机学院　重庆　400030)
[②](重庆大学软件学院　重庆　400030)
[③](重庆邮电大学软件学院　重庆　400067)

摘　要：在面向大规模化、强动态性、可靠性要求较高的网络节点间故障检测中，传统的故障消息传递模式会引起网络阻塞、时延不稳等问题，导致检测系统可扩展性变差，检测有效性降低。该文提出一种基于故障消息随机散播的自组织邻域检测协议 SONFDP。从自组织的思想出发构造了节点检测邻域，在每一邻域中自动生成用于域间检测的代理节点；设计了邻域内基于随机散播故障检测模式的检测算法，继而利用代理节点进行域间节点检测。另外，为防止故障消息随机散播时目标选择的盲目性，还设计了冗余消息避免机制，进一步减少了检测所产生的冗余故障消息数。对该协议的正确性进行了理论分析及证明，并在广域网环境中进行实验，结果表明 SONFDP 协议在避免泛洪引起网络拥塞的同时，能显著降低检测的系统耗费，增强传统故障检测方法的可扩展性和有效性。

关键词：动态网络；故障检测；自组织邻域；检测模式
中图分类号：TP302.8　　**文献标识码**：A　　**文章编号**：1009-5896(2010)09-2145-06
DOI: 10.3724/SP.J.1146.2009.01505

Self-organized Neighborhood Fault Detection Protocol under Dynamic Dependable Network Environments

Chang Guang-hui[①]　Chen Shu-yu[②]　Xu Guang-xia[①③]　Lu Hua-wei[①]
[①](*College of Computer Science*, *Chongqing University*, *Chongqing* 400030, *China*)
[②](*School of Software Engineering*, *Chongqing University*, *Chongqing* 400030, *China*)
[③](*College of Software Engineering*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400067, *China*)

Abstract: To implement fault detection under large-scale, strong dynamic, high reliability required network environments, the traditional fault message dissemination would encounter network congestion, latency instability etc.. A fault detection protocol based on self-organized neighborhood construction is proposed, and agent nodes are chosen to implement detection between neighborhoods. In every single zone, a random dissemination fault detection algorithm called Self-Organized Neighborhood Fault Detection Protocol (SONFDP) is designed. This protocol can avoid network congestion caused by flood, reduce the network overhead and extend the scalability of fault detection. Meanwhile, a mechanism of redundant message avoidance is designed to further reduce the number of messages generated by detection. SONFDP is proven to be correct and effective by relevant mathematical analysis and experiments.

Key words: Dynamic network; Fault detection; Self-organized neighborhood; Detection mode

1　引言

以因特网为代表的信息化网络已成为现代社会最重要的基础设施之一。以往的网络研究主要集中在信息传输的效率，网络功能的完善性，以及系统的可扩展性等方面，对于网络的安全可靠性没有引起足够的重视。然而网络故障，节点失效，恶意攻击等可靠性，安全性隐患的存在却导致网络服务不可信的严重后果[1,2]。如今网络服务面临的一个关键任务就是如何让用户得到可信赖的服务结果。正如美国工程院院士 David Patterson 教授所指出的：当今的计算机系统是想要建造高可信的网络服务[3]。

随着网格，P2P，传感器等大型网络化应用系统的快速发展，已经出现了基于网格，P2P，传感器网络的带故障检测的高可靠性应用系统[4−6]。传统的故障检测不再适应其大规模化、强动态性、传

2009-11-24 收到，2010-06-14 改回
科技部国际科技合作项目(2007DFR10420)和重庆市自然科学基金(2008BB2307)资助课题
通信作者：常光辉　cquteam@yahoo.com.cn

输时延不确定等特点。据此，研究人员提出了多种故障检测算法，同时也提出了对动态网络故障检测的新要求：协议或算法应当满足系统的动态性，可扩展性，低耗费，灵活性[7,8]。文献[9]提出基于灰模型的动态心跳故障检测方法，有效缩小了观测样本容量，但没有考虑心跳消息传播方式的问题，若系统规模扩大则该方法的有效性会随着网络耗费的增大而降低。文献[10,11]提出了以线性回归方法来预测故障时间间隔 Δt，较好地解决了分布式系统动态性的问题，但是其所需样本量较大，也存在网络耗费过大的问题。

Renesse提出了gossip-style的故障检测协议[12]，该协议利用了流言广播在网络中散播消息的高可靠性，并且能够避免泛洪广播消息引起的网络拥塞问题。但此方法的缺点是系统会产生过多的冗余信息，同样导致系统的可扩展性变差。对于系统耗费过大的的问题，文献[13]提出了一种寄生式故障检测算法，该算法能有效的降低系统消耗，并不额外产生探测信息，但检测组件与应用系统高度耦合，使该方法通用性变差。文献[14]采用故障检测的方法来确定网络节点的可信任值，这要求故障检测方法能精确快速地对故障定位，以适应网络节点可信任值的动态性。

本文提出基于自组织邻域的随机散播故障检测协议在构造自治邻域的基础上有效地利用了随机散播的可靠性，同时由于每个邻域相对自治，大大降低了探测所带来的通信消耗和时间损耗，使得协议具有高可扩展性和低耗费等特点。

2 系统模型及基本协议

2.1 系统模型描述

定义一个网络系统为包含有有限多个结点集 $\Pi=\{p_1,p_2,\cdots,p_i\}$，其中$i$>2且$i\in N$；集合中的$p_i$为网络系统中的一个组件或进程的抽象表示。

定义网络系统中的故障检测集为 $\Omega=\{d_1,d_2,\cdots,d_j\}$，其中$j$>2且$j\in N$；对于上面两个集合中的元素$p_i$，$d_j$：$\forall p_i\in\Pi$，$\exists d_j\in\Omega$，其中$i$=$j$；称$d_j$为依附于$p_i$的检测器。

假定 系统中任取网络节点集中的两个节点p_i和$p_j(i\neq j)$，它们之间具有概率为1的网络连通性，当且仅当系统中通信的两节点其中之一出现崩溃(crash)情形时才出现不能连通，这个假定其实是明确系统中的链路不存在故障。同时，系统中任意节点不存在Byzantine式故障。

2.2 随机散播检测基本协议

为系统中的n个节点都配备一个检测器d，它们形成一个检测集，其中$\forall p_i\in\Pi$，$\exists d_i\in\Omega, i\in N$。每个故障检测器将会维持一个视图View$_i$，视图中存有成员的ID(ID即成员的身份信息包含有地址信息)，健康节点集S_{health}，怀疑节点集$S_{\text{suspicion}}$，以及故障节点集S_{crash}，实现时可以采用一个结构体变量，另外视图中还有一个成员计数器beat counter，此计数器具有通常检测器的心跳数意义。

系统中每个节点的检测器，经过一个时间间隔T_{interval}，它自己将会主动把自己的信息随机发送给View中健康节点集或怀疑节点集里面的一个节点。发送时，节点p将自己的心跳计数beat counter自加一次。其他节点的检测器，收到此信息后，记录收到的时间戳last time，并设置怀疑时间间隔$T_{\text{suspicion}}$，随后等待下一次信息的到来。若在 last time + $T_{\text{suspicion}}$时刻仍然没有收到某一被检测点的更新心跳信息，或者收到的心跳信息不是beat counter +1，那么表明该节点可能发生了异常，则将会把该节点从S_{heath}中移入$S_{\text{suspicion}}$集合中。

但此时却不允许删除，若在$T_{\text{suspicion}}$之后将被检测点直接移除，则有可能导致错误。实际操作中，可以采用已有的各种基于时间预测的故障检测方法[9−11]计算出T_{out}的值。但这种方法通常需要较大的计算量来得出预测的时间，在系统资源紧张时甚至会带来算法的失效。另一种简单有效的做法可以采用设置移除时间T_{out}=2×$T_{\text{suspicion}}$。这样做的好处是不会使得系统中的某个故障节点的心跳消息持续逗留在系统中。

2.3 邻域构造方法

由前所述，如果可信系统规模扩大，那么网络节点间的故障探测就会导致消息量剧增，时延也会变得不能忍受，随之系统的误检测率也将随网络规模的扩大不断增加，引发检测方法程度性失效。为了解决这个问题，本文引入了自组织邻域的方法来对节点进行划分，使之形成较小规模的自治域，这样可以有效避免随网络规模扩大引发的上述缺陷。其构造过程如下：

算法1

步骤1 选取系统中的一个节点I对系统发出广播探测信息，信息数为N−1；

步骤2 每个存活的节点对此广播信息作出应答，初始节点在回收的时候对应答消息按时间排序，选取前$\lceil N/\delta\rceil-1$个节点，作为以初始节点为中心的一个邻域；

步骤3 排除掉已选取的$\lceil N/\delta\rceil-1$个节点，在剩余的节点中选取应答时延最长的节点作为下一个初始节点，重复步骤1，步骤2；

步骤4　当剩余节点数小于$\lceil N/\delta \rceil - 1$的时候结束循环。

在这里，N为系统总节点数，参数δ的值代表要划分的邻域的个数。在实际中可以根据$T_{\text{suspicion}}$来确定，因为如果在初始节点构造探测的应答时间已经超出了$T_{\text{suspicion}}$的范围，那么它已经可以作为一个可疑节点，然而既然有响应那么应答节点必定处于活动状态。如此说明包含初始节点 I 的邻域对其探测已经失效，这样反过来说明采用最长时延节点作为另外一个邻域的中心是合理的。

此算法中每次选取的邻域初始节点同时也是新生成邻域的代理节点。当有节点要散播自己的存活消息时，通过代理节点进行邻域间的消息散播。

推论1　当系统中的节点执行算法1时，在有限步内将划分为若干个邻域，且覆盖系统内所有节点。

证明　由以上步骤经过递推可知，此结论成立。

3　协议的分析与评估

3.1 检测协议的可靠性分析

本文提出的故障检测协议采用随机散播方式进行检测，首先分析单一邻域内的协议执行情况。

称系统中的节点收到其他节点存活信息为被感染。称系统经过一个T_{interval}时间为系统散播的一个轮次，记为r。设在第r轮系统中已经有λ_r个节点被感染，考察未被感染节点的将被感染的概率(当$r=0$时$\lambda_0=1$)。

考虑随机散播的执行过程，当某一个节点被感染后则会从它的本地视图中随机抽选出一个节点作为下一轮散播的对象，View中存储了自身邻域中的节点，邻域中包含的节点数是n，通过邻域构造之后，可以得知$n=\lceil N/\delta \rceil$，在单个邻域中，最简单的是从除自己外的节点中随机选一个，这样邻域中任一节点被i感染的概率为$1/(n-1)$，从而邻域中任一节点未收到i发出的探测消息的概率为$1-1/(n-1)$。既然邻域中已经有λ_r个节点被感染，那么很显然邻域中未被感染的节点在本轮仍不会被感染的概率应该是$(1-1/(n-1))^{\lambda_r}$。由此可以得出随机散播过程中，经过前r轮有λ_r个节点被感染的情形下，某个未被感染节点被感染的概率为

$$\rho(\lambda_r)=1-\left(1-1/(n-1)\right)^{\lambda_r} \tag{1}$$

从存活消息的散播方式可以看出，一个正准备散播消息的节点从其视图中选择了$n-1$个节点进行随机散播。但实际上在这$n-1$个节点中存在若干个节点已经得到了此消息的情况。这样，此协议必定会产生不必要的信息耗费。这是由于节点在散播时选择目标的盲目性决定的。所以我们可以考虑某种选择方式以降低散播的盲目性。

在本文中采用存储路由信息的方法对其改进。具体做法为：被感染节点进行下一轮散播时，将上一轮发送存活信息的节点嵌入到本次散播的消息中，并作记号Mark，标记为信息的途经节点。这样，在下一节点做下一轮散播选择的时候，消息曾经过的途径节点将被剔除。于是可得改进后的$\rho(\lambda_r)$为

$$\rho'(\lambda_r)=1-\prod_{i=0}^{\lambda_r}\left(1-1/(n-h_i-1)\right) \tag{2}$$

这里的h_i称为协议的避免因子，是在散播选择中被剔除掉的节点数。它的存在可以有效地削减协议随机散播带来的系统冗余消息，降低所谓的“乒乓效应”。

从以上的分析可以得出系统感染情况演化的迭代关系式为

$$\lambda_{r+1}=\lambda_r+(n-\lambda_r)\rho'(\lambda_r) \tag{3}$$

N为系统总节点数。

另外，系统中任一节点在第$r+1$轮收到探测消息的概率为λ_r/n，则所有节点在第$r+1$都被感染的概率为$(\lambda_r/n)^n$。设α为给定的检测覆盖率的阈值，则当

$$\alpha<(\lambda_r/n)^n \tag{4}$$

时，通过式(2)-式(4)可以计算经过多少轮次算法将满足系统检测的覆盖率α。

3.2 网络耗费以及检测时间相关分析

过大的网络耗费会使得网络负荷超载引起网络拥塞等问题。这一节分析本文所述协议的网络耗费问题。

根据式(3)所给出的$\rho'(\lambda_r)$的计算式，会使得后续的分析在数学处理上变得复杂。另外在实际的应用中有可能采用不同的避免“乒乓效应”的方法。因此可以近似的假设每一个节点的避免因子为一个h_i的期望值h。这样的假设不会给协议的本质带来变化。则式(2)变为

$$\rho(\lambda_r)=1-\left(1-1/(n-h-1)\right)^{\lambda_r} \tag{5}$$

将其代入式(3)则

$$\lambda_{r+1}=n-(n-\lambda_r)\left(1-1/(n-h-1)\right)^{\lambda_r}$$

可以得到

$$\frac{n-\lambda_{r+1}}{n-\lambda_r}=\left(1-1/(n-h-1)\right)^{\lambda_r}$$

因为$(n-h-1)$远小于1，上式近似于：

$$\frac{n-\lambda_{r+1}}{n-\lambda_r}=e^{-\lambda_r/(n-h-1)} \tag{6}$$

进一步可得

$$\lambda_r=(n-h-1)\ln\left(n-\lambda_r/(n-\lambda_{r+1})\right) \tag{7}$$

从协议散播的方法可知第 r 轮在系统中所产生的消息数就是 λ_r，所以系统中直到覆盖完成的第 $r+1$ 轮所产生的消息数

$$\theta = \sum_r \lambda_r = \sum (n-h-1)\ln(n-\lambda_r/(n-\lambda_{r+1})) \quad (8)$$

所以消息数 θ 为 $(n-h-1)\ln(\mathrm{n}-1)$。

引理 设系统总节点数为 N，采用随机散播方式传播存活消息的系统总耗费数为 $(N-h-1)\cdot\ln(N-1)$。

证明 由以上分析直接可以得出结论。

定理1 基于随机散播的分邻域检测方法在通信耗费上必定优于单一集合的故障检测方法。

证明 设系统集合 Π 中总节点数为 N，由式(8)可知，采用随机散播的检测方法系统中产生的消息数 θ 为 $(N-h-1)\ln(N-1)$。

若将其划分为几个彼此相近的邻域集合 $\Pi_1, \Pi_2, \cdots, \Pi_n$，对每个子集合中的节点也做随机散播的故障检测，则邻域子集的通信耗费 θ_i 为 $(\lceil N/\delta \rceil - h - 1)\ \ln\left(\lceil N/\delta \rceil - 1\right)$。

在邻域检测中总的耗费为

$$\theta' = \sum_{i=1}^{\delta} \theta_i \quad (9)$$

因为通过算法1划分邻域时，存在最后一个邻域中节点数目小于 $\lceil N/\delta \rceil$ 的情况，所以由式(9)可以推导出：

$$\theta' \le \delta\left(\lceil N/\delta \rceil - h - 1\right)\ln\left(\lceil N/\delta \rceil - 1\right) \quad (10)$$

同时，$\lceil N/\delta \rceil \le N/\delta + 1$，代入式(10)，得 $\theta' \le (N - \delta h)\ln\left(\lceil N/\delta \rceil - 1\right)$。

根据前述邻域划分方法，δ 必为大于1的正整数，故可得

$$(N-h-1)\ln(N-1) > (N-\delta h)\ln\left(\lceil N/\delta \rceil - 1\right)$$

由此可知 $\theta' < \theta$。 证毕

定理2 基于随机散播的分邻域检测方法在时间耗费上必定优于单一集合的故障检测方法。

证明 设系统总节点数为 N，则邻域子集内节点总数必然小于 N。分析协议本身，其检测消息的散播基于轮次的概念，设未划分邻域的系统检测在第 r 轮覆盖所有节点。根据3.1节中式(3)：$\lambda_{r+1} = \lambda_r + (N-\lambda_r)\rho'(\lambda_r)$，其中 $(N-\lambda_r) > 0$，且传染概率 $\rho'(\lambda_r) > 0$; 则必然有 $\lambda_{r+1} > \lambda_r$; 所以系统中节点的被感染数 λ_r 必定为关于轮次 r 的离散单调递增函数。

由单调函数的性质可知：当 $\lambda > \lambda'$ 时其对应的轮次也必定有如下关系 $r > r'$。故此感染系统总节点数为 N 的节点所耗费的轮次必定大于感染其邻域子集的轮次。而分领域随机散播检测的情况下，对某个邻域子集的检测时间等于对全集检测的时间。

证毕

4 实验结果

本文利用Socket网络编程API在Linux系统上开发了网络故障探测工具。并采用它在广域网络环境下仿真随机散播故障检测，以对本文所提协议的若干结论及有效性进行验证。邻域内消息散播采用UDP方式，邻域间则采用TCP方式。

4.1 SONFDP协议对系统内节点的检测覆盖性试验

选取16个节点作为实验床，节点操作系统采用Linux2.6.20内核版本，100 M的网络接入带宽。每一个节点上开辟 $N/16$ 个故障检测线程进行模拟仿真随机散播实验。每个线程都有 r 轮次的变量，另外为了设置 T_{interval}，需要在每个线程配置一个Timer对象，用于控制节点发送检测消息的时间间隔，实验中取400 ms。实验监测随着轮次 r 的变化检测协议在系统中感染节点的覆盖情况。模拟的系统感染曲线如图1所示。

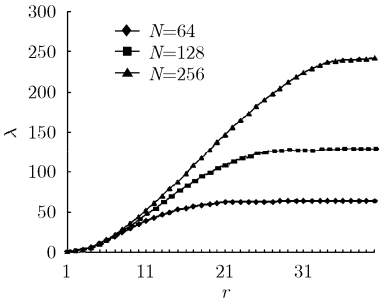

图1 系统感染数变化曲线

由图1可以看出，对于不同规模的系统节点，前5轮感染曲线的斜率较小，随后逐渐增大，到后期又逐渐降低。说明随机散播协议对系统节点的感染为慢启动过程，这可以有效的避免泛洪引起的网络拥塞。另外，不同系统规模下执行此协议的节点覆盖率对比情况，如表1所示。

从表1 中的数据可以看出，随着系统规模的扩大，探测的覆盖率和时间的比值大大减小。取阈值 $\alpha = 0.95$，当 N=64，r=20时，覆盖率 $\alpha > 0.95$；当

表 1 不同轮次系统感染节点覆盖率对比

r	5	10	15	20	25	30	35	40
N=64	0.16	0.55	0.93	0.97	1	–	–	–
N=128	0.09	0.36	0.59	0.86	0.97	1	–	–
N=256	0.05	0.18	0.33	0.52	0.68	0.85	0.94	0.96

N=128时，r=25时，$\alpha > 0.95$；而反观N=256的情形，直到第40轮才有覆盖率达到阈值要求。这充分说明系统规模越大探测在时间耗费上效果越不理想，同时也证实了本文基本思想的正确性。

4.2 SONFDP协议网络耗费对比

实验以重庆大学的两个实验室以及电子科技大学一个实验室作为实验床。其中每个实验室取8个节点，每个节点运行8个故障检测线程，总仿真节点数为192，探测阈值取$\alpha = 0.95$。由于实际网络使用的情况会随着时段的不同有较大差异，本实验取两个时段，日间和夜间分别做3组相同实验，同样的考虑取略长的散播时间间隔$T_{\text{interval}} = 600$ ms。

根据2.3节的邻域构造方法，选取δ=3，则可得3个邻域的节点拓扑，每个邻域用δ_i表示。在每个模拟线程中增设一个消息接受计数器C_i，节点每收到一个消息则其计数器加1。在系统达到探测的阈值时，则可计算系统总的耗费为

$$C = \sum_{i=1}^{192} C_i$$

实际计算时先在每个邻域中计算总的耗费，然后将每个邻域的消息总数相加即得系统总耗费。

对比实验结果如表2所示。

表2 4种方法的系统耗费及误测率对比

P	G							
	1	2	3	4	5	6	$\bar{C}$	e
SONFDP	819	856	923	792	813	756	826	0.09
Renesse	1228	1356	1303	1084	1101	1205	1212	0.16
Flood	182	168	171	183	179	182	177	0.36
Ji xiaobo	190	187	177	191	180	185	184	0.14

表2中G表示实验组别，P表示检测协议，$\bar{C}$为平均耗费，e为误检测率。从表2可以看出，SONFDP检测协议在网络耗费方面比文献[12]的检测方法减少了31%；在误检测率方面比文献[12]以及文献[9]中的方法分别降低了7个百分点和5个百分点。网络耗费减少的原因由3.2节的分析可知。而误检测率低的原因是，SONFDP所划分邻域内的节点所处网络状况相对稳定，网络时延也较短，这对于检测时间的预测非常重要，所以即便在白天网络使用高峰期其误报率仍然较低。Flood方法尽管在通信量有很大的优势，但在检测有效性方面与上述两种方法的差距同样很大，尤其是在网络使用高峰时，它引起的网络拥塞使得丢包率和消息传递时延过大，致使其变的几乎不可用。

5　结束语

本文根据可信网络服务的大规模化，高动态性，消息传递时延不确定性等特点，提出了SONFDP故障检测协议。采用自组织划分邻域的思想建立了一种高效可扩展的故障检测方法，仿真实验表明：SONFDP可以有效地控制故障检测时的冗余网络耗费，并且在时间上也有较为明显的优势。由于这两方面性能的提高，从而使得故障检测时间易于预测，进一步增强了故障检测的可靠性。

下一步的研究工作是如何建立更加合理有效的自组织检测邻域。根据故障检测和可信服务的特点分析自治域的划分方法，以期使得检测协议的服务对象更具有针对性，检测耗费进一步降低，将其应用于具有可信性的网格，P2P等大型网络化应用系统。

参 考 文 献

[1] 林闯，彭学海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751–758.
Lin Chuang and Peng Xue-hai. Research on Trustworthy Networks[J]. *Chinese Journal of Computers*, 2005, 28(5): 751–758.

[2] 闵应华. 网络容错与安全研究评述[J]. 计算机学报, 2003, 26(9): 1035–1041.
Min Ying-hua. Coments on basic research of reliable and Secure Networks[J]. *Chinese Journal of Computers*, 2003, 26(9): 1035–1041.

[3] Patterson D. Recovery oriented computing. Presented at Princeton University [EB/OL]. 2002, http://roc.cs.berkeley.edu /talks/UIUC.ppt.

[4] Yamanouchi M, Matsuura S, and Sunahara H. A fault detection system for large scale sensor networks considering reliability of sensor data[C]. Proc of the Ninth Annual International Symposium on Applications and Internet (SAINT'09). Seattl, USA, 2009: 255–258.

[5] Lee H M, Park D S, and Hong M, *et al*.. A resource management system for fault tolerance in grid computing[C]. Proc of International Conference on Computational

Science and Engineering (CSE'09). Vancouver, CA, 2009, 2: 609–614.

[6] Chtepen M, Claeys F, and Dhoedt B, *et al*.. Adaptive task checkpointing and replication: toward efficient fault-tolerant grids[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2009, 20(2): 180–190.

[7] Jain A and Shyamasundar R K. Failure detection and membership in grid environments [C]. Proc of the 5th IEEE/ACM Int'l Workshop on Grid Computing (GRID'04), Los Alamitos, CA, IEEE Computer Society Press, 2004: 44–52.

[8] Hwang S and Kesselmanl C. A flexible framework for fault tolerance in the grid [J]. *Journal of Grid Computing*, 2003, 1(3): 251–272.

[9] 姬晓波，陈蜀宇，田东，等. 高效可扩展的网格系统动态故障检测算法[J]. 武汉大学学报(信息科学版). 2008, 33(10): 1046–1050.
Ji Xiao-bo, Chen Shu-yu, and Tian Dong, *et al*.. An efficient and scalable fault detection algorithm for grid systems[J]. *Geomatics and Information Science of Wuhan University*. 2008, 33(10): 1046–1050.

[10] Chen W, Toueg S, and Aguilera1 M K. On the quality of service of failure detectors [J]. *IEEE Transactions on Computers*, 2002, 51(2): 13–32.

[11] Hayashibara N, Défago X, and Yared R, *et al*.. The ϕ accrual failure detector[C]. Proc of the 23rd IEEE Int'l Symp on Reliable Distributed Systems(SRDS'04), Los Alamitos, CA, IEEE Computer Society Press, 2004: 66–78.

[12] Renesse R, Minsky Y, and Hayden M. A gossip-style failure detection service[C]. Proceedings of International Conference of Distributed Systems Platforms and Open Distributed Processing (IFIP), The lake district, UK, Springer-Verlag Press, 2009: 55–70.

[13] 左朝树，刘心松，邱元杰，等. 一种分布式并行服务器节点故障检测算法[J]. 电子科技大学学报. 2007, 36(1): 119–122.
Zuo Chao-shu, Liu Xin-song, and Qiu Yuan-jie, *et al*.. A node fault detection algorithm in distributed parallel server[J]. *Journal of University of Electronic Science and Technology of China*, 2007, 36(1): 119–122.

[14] 纪俊杰，阳小龙，王进，等. 基于信任关系的 IP 网络容错容侵机制[J].电子与信息学报. 2009, 31(7): 1576–1581.
Ji Jun-jie, Yang Xiao-long, and Wang Jin, *et al*.. An efficient fault-tolerant and intrusion-tolerant scheme based on trust relationship for IP networks[J]. *Journal of Electronics & Information Technology*, 2009, 31(7): 1576–1581.

常光辉： 男，1980 年生，博士生，研究方向为可信计算、容错、分布式计算.

陈蜀宇： 男，1963 年生，教授，博士生导师，研究方向为容错计算、网络与分布式计算.

徐光侠： 女，1974 年生，副教授，研究方向为可信计算.