doi:10.11959/j.issn.1000-436x.2015081

可重构网络的可用性模型

赵靓，张校辉，王雨
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对网络故障恢复机制可以对可重构网络性能产生重要影响的实际情况，从理论上对可重构网络的运行状态进行分析，提出了一种可重构网络的可用性模型。该模型以节点服务能力和网络服务能力的量化描述为基础，通过引入可重构网络的状态转移理论，以有限状态马尔科夫链进行理论分析得到。通过仿真实验对该可用性模型的有效性进行验证，仿真结果表明，理论模型计算结果与仿真结果拟合性较好，可用于描述特定可重构网络的可用性能。

关键词：可重构网络；节点服务能力；网络服务能力；可用性模型
中图分类号：TP393 **文献标识码**：A

Avaliability model for reconfigurable network

ZHAO Liang, ZHANG Xiao-hui, WANG Yu
(National Digital Switching System Engineering and Technology Research Center, Zhengzhou 450002, China)

Abstract: For network fault recovery mechanisms can have a significant impact on network performance reconfigurable actual situation theoretically analyze the running reconfigurable networks, a reconfigurable network availability model is proposed. In this model, quantitative description of the node service capabilities and network services capabilities, based on reconfigurable network by introducing state transition theory, finite-state Markov chain theoretical analysis. To verify the validity of the availability of the model by simulation, simulation results show that the theoretical model calculations and simulation results fit better, can be used to describe the specific performance reconfigurable networks available.

Key words: reconfigurable network; node service capability; network service capability; avaliability model

1 引言

可重构柔性网络理论[1~3]主要研究在实现网络资源高效利用的基础上如何面向用户的应用需求提供差异化网络服务。在该技术体系中，根据面向服务的网络分层模型，采用“业务-服务-构件”映射技术将网络资源构件化；从用户业务可规划和网络资源可管理角度出发，将网络服务划分为公共服务、个性服务和即时服务，采用平台化支撑构件化处理的节点重构技术，可动态构建满足服务需求的可重构服务承载网[4,5]（RSCN, reconfigurable service carrying network）；根据服务需求的变化，采用主动式资源管理技术调整网络资源分配，使网络资源分配与用户需求相匹配，从而实现网络资源的高效利用。综上，RSCN 的相关研究内容就是以如何满足差异化服务需求为目标提出的。然而，现有相关研究在讨论 RSCN 进行描述的，重点在于为不同种类的服务提供所需的带宽等基础网络资源，以保障通信业务的基本需求得以满足，而对于其安全属性的需求则关注不足。事实上，差异化的安全属性也应是差异化服务需求的重要内容之一，例如，提供娱乐服务的承载网与提供金融服务的承载网在安全属性方面的需求显然是不同的。因此，在讨论 RSCN 如何提供差异化服务时不能仅考虑业务性能方面的需求，还必须充分考虑其安全性能的需求。

网络安全性通常被理解为在受到恶意攻击时

收稿日期：2013-12-24；**修回日期**：2014-03-10
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2012CB315901, 2012CB315905）
Foundation Item: The National Basic Research Program of China (973 Program) (2012CB315901, 2012CB315905)

计算机网络性能指标的反应。目前，普遍关注的网络安全性包括 6 个基本属性，包括可用性、可靠性、保险性、可行性、完整性、机密性[6,7]。事实证明，想要构建绝对安全的网络系统，在网络应用中满足上述所有安全属性的要求不论是从技术实现上来说，承载差异化服务时是从业务属性出发还是从成本核算上来说都是不切实际的[8]。因此，必须明确网络服务的安全属性需求，并根据其定量描述的安全性能有针对性的构建网络安全机制和措施才能针对特定的网络业务提供最好的安全服务。

在上述安全属性中可用性是对网络系统有效和无效交替变化过程的一种量化，并着重描述网络系统正常运行的可能性，因此是网络系统最基础、最重要的安全属性之一[9]。综上，本文主要研究承载各类差异化服务的 RSCN 的的可用性模型。为了定量描述网络系统的可用性能，首先从理论上对可重构网络的运行状态进行分析，给出网络系统的有效和无效状态的界定条件，由此构建可重构网络系统的状态可达图；然后提出一种用以定量描述节点和网络系统性能的描述方法，并以此为基础对上述状态可达图进行理论分析，最终得到可重构网络的可用性模型。最后通过仿真试验结果验证上述可用性模型的准确性。

2　相关工作

目前针对网络安全模型方面，国内外有很多的研究成果。陈秀真等[10]基于 IDS 海量报警信息和网络性能指标，结合服务、主机本身的重要性及网络系统的组织结构，提出一种层次化安全威胁态势量化评估模型及其相应的计算方法。该方法的问题在于必须针对特定的攻击类型进行评估，对未知攻击无法评估，而且评估是在攻击发生以后进行，局限性较大。

姜伟[11]，McDermott J[12]等基于攻防博弈理论，提出了网络防御图模型、攻防策略分类及其成本量化方法，并基于上述研究提出一种最优主动防御选取算法，其主要目标是建立最优的防御策略，用以保证网络安全。冯萍慧等[13]在安全评估中引入可靠性理论，对分布式系统的脆弱性进行分析和量化评估，为增强分布式系统的安全性提供理论依据。上述模型都可以归类为一种防御模型，目标是分析系统的弱点并进行主动防御，而对于网络受到攻击以后的恢复则没有考虑。

事实上，对于网络系统来说，想要防御所有的攻击是不可能的，再精良的防御策略也只能是各种安全措施的一部分，除了加强防御以外，还必须考虑系统的应急恢复机制，这也是网络系统安全机制的重要组成部分。但是，当前对网络设备故障的诊断与处理仍然需要人工干预，根据网络系统受攻击的范围、网络节点的故障情况、发现服务失效时的响应机制不同，其恢复手段和时间也不同，难以进行定量分析，从而无法评估故障恢复对网络系统可用性的影响，因此现有的网络安全模型也通常对故障恢复时间等性能参数进行忽略。而可重构服务承载网(RSCN)本质上可以概括为是通过可重构技术构建的虚拟网，其本身具备的可重构功能不仅是构建网络系统的基本方法，亦是网络故障恢复的重要手段。正是由于 RSCN 采用了可重构技术，使其在网络故障恢复方面具有先天的优势，能够在一定程度上保证故障恢复的时间性能。因此，在对 RSCN 的可用性进行评估时，应该充分考虑故障恢复对可用性性能的影响，而上述网络安全模型对此没有定量分析，因此不适用于 RSCN 的可用性评价。因此，本文提出面向 RSCN 的基于故障恢复机制的可用性模型，从而为系统度量可重构网络系统的安全性能提供理论依据。

3　可重构网络状态

网络系统是一个复杂的系统[14]，其节点状态、链路状态等网络设备状态随时都在改变，进而影响整个系统的运行状态，而造成上述设备状态改变的因素主要有软硬件错误、人为错误、自然灾害、恶意攻击等。如果把上述触发系统状态改变的诱因都当作随机事件，则在保证设备可靠性的前提条件下，显然前几种随机事件发生的概率很小，且相互独立，从而产生的结果也是可控的；而恶意攻击作为一种人为有意识的破坏活动，相比于其他触发条件其发生概率更高，且互相不独立，往往会产生多设备状态同时或相继改变的连锁反应，从而对网络系统造成严重的后果，甚至造成网络系统失效。

为了简化分析过程，本文假设网络系统的失效都是由网络攻击造成的，而对于一般的网络攻击，网络设备具备一定的防御攻击的能力。另外，链路作为与节点相关的网络资源，本文不单独讨论其状态改变对系统的影响，所以文中所述的攻击都是指节点受到的攻击。一旦对攻击的防御失败，即发生

一次成功的节点攻击，则该节点所有功能失效，通过反馈机制网络管理中心能够探测到节点失效状态，并进行相应的故障恢复处理，而从节点失效到网管中心探测到节点失效，并最终将节点恢复到正常状态需要一定的时间，在此周期内，如果相继发生节点失效事件，且失效节点累计到一定程度，则引起整个网络系统失效。正如本文前面提到的，可重构网络中通过重构机制对失效的网络系统进行恢复，由于重构过程会影响网络服务提供，因此当网络系统进行重构时停止提供所有服务，即处于失效状态，而处于其他状态时，则正常提供服务。

基于上述假设，可重构网络系统的运行状态转移过程可分解为网络状态在遭受攻击时的一系列转移步骤。本文将可重构网络系统的运行状态描述为 3 个状态，分别为正常状态（Normal）、攻击防御状态（Prevention）、重构状态（reConfiguration），如图 1 所示。

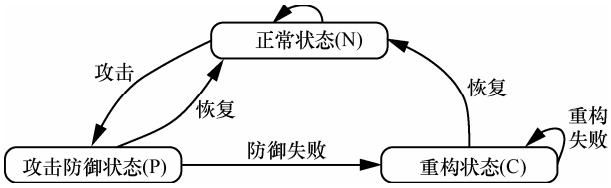

图 1 可重构网络状态转移

其中，正常状态(N)是指网络系统能够提供正常服务的状态，是网络系统中各种安全机制作用后的目标状态；攻击防御状态(P)是指从发生攻击开始到检测出攻击并进行响应的状态；重构状态(C)是指攻击检测或攻击响应失败的情况下进入的状态，在该状态下根据服务失效发生的情况提出重构请求，并利用重构机制使网络系统从服务失效状态恢复到正常状态的过程。当系统处于前 2 个状态时，网络系统可以满足服务能力需求，即网络系统处于有效状态；而处于第 3 种状态时，其服务不可用，系统处于失效状态。

根据上述状态转移图，定义可重构网络系统的状态空间为 $S=\{N,P,C\}$。基于上述假设和描述，并根据可重构网络系统状态转移过程，可以得出可重构网络系统中不存在吸收状态，均为瞬时状态，且所有的瞬时状态可分为可用状态和不可用状态，即可重构网络系统不存在永远可用的状态，也不存在永远不可用的状态。根据状态空间中各元素的状态类型，状态集 $W=\{N,P\}$ 表示系统可用状态集；状态集 $I=\{C\}$ 表示系统不可用状态集。因此，可重构网络系统的状态空间也可以表示为 $S=W\cup I$。

根据系统可用性的定义，构建满足特定可用性服务需求的 RSCN 的目标就是能够使网络在其运行生命期中满足特定比率的时间停留在状态集 W，换言之，为了提高可重构网络的可用性就要尽可能减小防御失败而进入状态集 I 的概率，并提高从状态集 I 恢复到状态集 W 的概率。假设 $\Pi=(\pi_N,\pi_P,\pi_C)$ 是 RSCN 系统处于各状态的稳态概率向量，π_k 为系统处于 k 状态的稳定状态概率，$W\subseteq S$ 是系统处于有效状态的概率集合，则 RSCN 稳态可用性的定义可以描述如下。

定义 1 （RSCN 稳态可用性）。成功构建的 RSCN 长期运行过程中，系统有效运行的时间与总运行时间的比值称为 RSCN 稳态可用性。有效运行时间的比例也可以表示为 RSCN 系统处于有效状态的稳定概率之和，其数学描述为

$$A_{\mathrm{RSCN}}=\sum_{k\in W}\pi_k \tag{1}$$

4 服务能力描述

要定量描述网络可用性指标，需要对网络状态及其转移条件进行定量描述。从用户角度出发，网络是否能够满足特定的服务需求是衡量网络是否有效的标准，因此本文从网络服务能力的角度对网络状态及其转移条件进行定量描述。

4.1 服务能力的概念

构建网络的目的是向用户提供特定的网络服务能力，而构建出来的网络是否能够满足用户需求需要一定的衡量标准，本文用服务能力描述网络满足特定服务需求的能力。

网络是由提供特定功能的网络节点构成的，用 $e_j(f)$ 表示节点 j 基于特定功能 f 的服务能力，记为 e_j；$\boldsymbol{P}_j=(f,c,i)$ 表示网络节点 j 的属性向量，P_i^f 表示在网络系统中，针对用户的特定服务需求，节点 j 所应该具有的功能；P_j^c 表示节点 j 相对应于 f 功能的实现能力；P_j^i 表示节点 j 在重构网络系统中 f 功能的输出能力，即通信能力，则节点服务能力定义如下。

定义 2 （节点服务能力）。网络节点能够向用户提供特定功能的能力，是用以判断网络节点是否可用的衡量标准，由功能(Function)、功能实现能力(Capability)及功能输出能力(Interface)3 个属性描述。其数学描述为

$$e_j(f) = P_j^f P_j^c P_j^i \tag{2}$$

基于上述定义，如果某节点在重构网络系统中具有 m 个接口，则其通信能力为各接口能力的总和，即 $P_j^i = P_j^{i_1} + P_j^{i_2} + \cdots + P_j^{i_m}$。

图 2 给出一个节点属性描述的例子，图例中具有功能 f 的节点 a~e 构建了一个满足需求的可重构服务承载网，其中节点 a 的属性为 $P_a^f = 1$，$P_a^c = 30$，$P_a^i = 10+20+30$；节点 b 的属性为 $P_b^f = 1$，$P_b^c = 30$，$P_b^i = 10+50$。

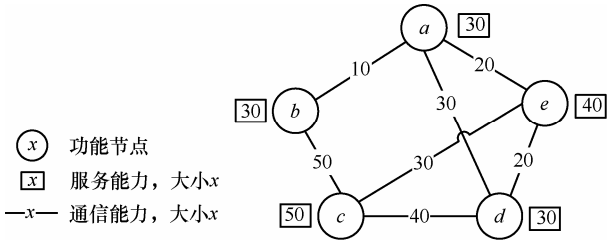

图 2　网络系统中的节点属性示例

用 $e_\Gamma(f)$ 表示网络系统 Γ 基于特定功能 f 的服务能力，记为 e_Γ；假设网络系统中有 n 个节点，则网络的服务能力即为 n 个节点服务能力的总和，由此给出网络服务能力的定义如下。

定义 3　（网络服务能力）。衡量网络系统面向特定的用户需求能够提供的基于某项功能的能力度量，是构成该网络系统的各网络节点服务能力的总和。对于一个具有 n 个节点的网络系统，其网络服务能力的数学描述为

$$\mathrm{e}_\Gamma(f) = \sum_{j=1}^{n} e_j(f) \tag{3}$$

4.2　基于服务能力的可重构网络状态描述

在进行网络重构时，要根据用户的服务需求对各节点属性提出具体要求。

1) 节点 j 要么具有相应的功能属性 f，要么不具有该功能属性，因此其取值为布尔值，即 $P_j^f \in \{0,1\}$。

2) P_j^c 根据用户需求，其有效取值空间为 $P_j^c \in [l_c, h_c]$。当功能实现能力 $P_j^c < l_c$ 时，则节点 j 失去功能属性 f 实现的能力，此时 $P_j^c = 0$。

3) P_j^i 根据用户需求，其有效取值空间为 $P_j^i \in [l_i, h_i]$，当通信能力 $P_j^i < l_i$ 时，则节点 j 失去功能属性 f 的输出能力，此时 $P_j^i = 0$。

根据式(2)，可以得出理论上可重构网络系统 Γ 中的基于某功能 f 的节点 j 的最大服务能力为

$$e_j(f)_{\max} = P_j^f P_j^c P_j^i = 1 h_c h_i，\text{记为 } e_{j\max} \tag{4}$$

假设可重构网络系统 Γ 由 n 个节点构成，则网络系统 Γ 基于功能 f 的最大服务能力为

$$e_\Gamma(f)_{\max} = \sum_{j=1}^{n} e_{j\max}，\text{记为 } e_{\Gamma\max} \tag{5}$$

基于上述描述，第 3 节中的网络系统各运行状态都可以用网络服务能力来进行量化描述。如果用 e_Γ 表示网络系统 Γ 的运行状态，$e_{\Gamma normal}$ 表示网络系统 Γ 能够处于状态 N 的最小网络服务能力，$e_{\Gamma fail}$ 表示网络处于有效状态的最小网络服务能力，则处于状态 N 的网络系统 Γ 可以描述如下

$$e_{\Gamma normal} < e_\Gamma < e_{\Gamma\max} \tag{6}$$

同理，处于状态 P 的网络系统 Γ 可以描述为

$$e_{\Gamma fail} < e_\Gamma < e_{\Gamma normal} \tag{7}$$

处于状态 C 的网络系统 Γ 可以描述为

$$e_\Gamma < e_{\Gamma fail} \tag{8}$$

由于网络中各种不确定因素的影响，节点不可能总是处于最大服务能力状态，为了方便讨论，假设某网络节点 j 基于功能 f 提供的服务能力要么为最大，要么无服务能力，即 $e_j \in \{0, e_{j\max}\}$；且用于构建可重构网络 Γ 的各节点具有相同的最大服务能力。基于上述假设，网络系统 Γ 的状态可以由基于网络服务能力的描述进一步转化为网络系统中可用节点数量的描述。用 k_Γ 表示当前网络 Γ 中可用的节点数量；$k_{\Gamma\max}$ 表示网络系统处于最大服务能力时正常提供服务的网络节点的数量；$k_{\Gamma normal}$ 是网络能够处于状态 N 而正常提供服务的网络节点的最小数量；$k_{\Gamma fail}$ 是网络处于有效状态时提供服务的最小网络节点数量，则网络系统处于状态 N 可以描述为

$$k_{\Gamma normal} < k_\Gamma < k_{\Gamma\max} \tag{9}$$

同理，网络系统 Γ 处于状态 P 和状态 C 分别可以描述为

$$k_{\Gamma fail} < k_\Gamma < k_{\Gamma normal} \tag{10}$$

$$k_\Gamma < k_{\Gamma fail} \tag{11}$$

上述各参数可以通过网络服务能力计算如下

$$k_{\Gamma\max} = \frac{e_{\Gamma\max}}{e_{j\max}}, k_{\Gamma normal} = \frac{e_{\Gamma normal}}{e_{j\max}}, k_{\Gamma fail} = \frac{e_{\Gamma fail}}{e_{j\max}} \tag{12}$$

根据用户对网络服务可用性需求的不同，可以定义不同的 $e_{\Gamma normal}$ 和 $e_{\Gamma fail}$，从而计算得到相应的 $k_{\Gamma normal}$ 和 $k_{\Gamma fail}$ 值。

5 可用性模型

可重构网络具有故障自动恢复能力，能够在网络发生故障时，通过自身的重构机制迅速发现故障点并及时进行恢复处理，这为可用性分析中故障恢复部分的定量描述提供了可能。但是，根据重构网络的规模、网络负载以及故障恢复算法等因素的影响，其故障恢复速度和成功率存在差异，因此故障恢复的相关参数影响整个网络系统的可用性；另外故障发生的频率和规模也会对系统可用性产生影响，因此在讨论可重构网络系统的可用性能时，还应该重点研究故障发生的相关参数。基于上述分析，对可重构网络系统可用性进行描述。

5.1 状态转移概率

基于服务能力的描述，可以对可重构网络的状态进行描述，也可以对状态间的转移过程进行描述。设 $p_{ij}(i,j\in S)$ 为发生事件时网络系统中从状态 i 到状态 j 的转移概率，这里的事件具体包括：节点受到攻击、成功防御节点攻击和失去服务能力的节点进行重构。由此，可重构网络系统Γ的一步转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix} p_{NN} & p_{NP} & 0 \\ p_{PN} & p_{PP} & p_{PC} \\ p_{CN} & 0 & p_{CC} \end{bmatrix} \tag{13}$$

假设可重构网络系统Γ中节点受攻击的概率与其权重成正比，而节点权重与其服务能力成正比，根据假设条件，可重构网络系统Γ中各节点受攻击概率相同，且与网络规模相关。假设网络系统中有 n 个节点，则各节点受攻击概率为

$$p=\frac{e_{j\max}}{e_{\Gamma\max}}=\frac{e_{j\max}}{me_{j\max}}=\frac{1}{n} \tag{14}$$

为了简化分析，进一步假设网络系统中各节点攻击成功的概率、节点成功防御的概率以及节点重构成功的概率分别独立，且与其节点权重成正比。

根据假设条件，网络系统Γ中节点攻击成功的概率 ρ，检测出单个节点攻击并成功防御节点攻击的概率 σ，以及受攻击失去服务能力后通过重构操作恢复节点服务能力的节点重构成功概率 γ 分别相等。

根据式（14），可知同时受攻击的节点数量 i 满足二项分布，即 $i\sim B(n,\rho)$，因此由德莫佛-拉普拉斯定理可知，$q_i=\dfrac{i-n\rho}{\sqrt{n\rho(1-\rho)}}$ 近似正态分布，由此可得到同时 i 个节点受攻击失去服务能力的概率向量为

$$\begin{aligned}\boldsymbol{Q}&=\{q_1,\cdots,q_i,\cdots,q_m\}\\&=\left\{\frac{1-n\rho}{\sqrt{n\rho(1-\rho)}},\cdots,\frac{i-n\rho}{\sqrt{n\rho(1-\rho)}},\cdots,\frac{n-n\rho}{\sqrt{n\rho(1-\rho)}}\right\}\end{aligned} \tag{15}$$

根据基于服务能力的网络状态描述，转移概率 p_{NN} 即是指处于状态 N 的网络系统在节点受到攻击的情况下仍然处于状态 N 的概率。而当受攻击失去服务能力的节点数量 $i<k_{normal}$ 时，网络系统均处于状态 N，此时网络系统最多可以再有 k_{normal}-i 个节点受到攻击而仍然处于状态 N，即

$$\sum_{j=0}^{k_1-i}\mathrm{C}_{m-i}^{j}\rho^{j}(1-\rho)^{m-i-j} \tag{16}$$

由网络系统状态描述可知网络系统处于状态 N 有 k_{normal} 种情况，因此在式(16)的基础上，根据式(15)，可得条件概率 p_{NN} 为 k_{normal} 种情况下发生状态转换的概率之和，即

$$p_{NN}=\sum_{i=0}^{k_1}\left(q_i\sum_{j=0}^{k_1-i}\mathrm{C}_{n-i}^{j}\rho^{j}(1-\rho)^{n-i-j}\right) \tag{17}$$

同理，可得条件概率 p_{NP} 为失去服务能力的节点数量 $i<k_{normal}$ 时，最少有 $k_{normal}+1-i$ 个节点再次受到攻击，最多有 n-i 个节点再次受到攻击的概率。同理可分别得到基于服务能力的状态转移概率。由此可重构网络系统Γ的一步转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix} \sum\limits_{i=0}^{k_1}\left(q_i\sum\limits_{j=0}^{k_1-i}\mathrm{C}_{n-i}^{j}\rho^{j}(1-\rho)^{n-i-j}\right) & \sum\limits_{i=0}^{k_1}\left(q_i\sum\limits_{j=k_1+1-i}^{n-i}\mathrm{C}_{n-i}^{j}\rho^{j}(1-\rho)^{n-i-j}\right) & 0 \\ \sum\limits_{i=k_1+1}^{k_2}\left(q_i i\sum\limits_{j=i-k_1}^{i}\mathrm{C}_{i}^{j}\sigma^{j}(1-\sigma)^{i-j}\right) & \sum\limits_{i=k_1+1}^{k_2}\left(q_i\sum\limits_{j=0}^{k_2-i}\mathrm{C}_{n-i}^{j}\rho^{j}(1-\rho)^{n-i-j}\right) & \sum\limits_{i=k_1+1}^{k_2}\left(q_i\sum\limits_{j=k_2+1-i}^{m-i}\mathrm{C}_{n-i}^{j}\rho^{j}(1-\rho)^{n-i-j}\right) \\ \sum\limits_{i=k_2+1}^{n}\left(q_i i\sum\limits_{j=i-k_1}^{i}\mathrm{C}_{i}^{j}\gamma^{j}(1-\gamma)^{i-j}\right) & 0 & \sum\limits_{i=k_2+1}^{n}\left(q_i\sum\limits_{j=0}^{i-k_1-1}\mathrm{C}_{i}^{j}\gamma^{j}(1-\gamma)^{i-j}\right) \end{bmatrix} \tag{18}$$

5.2　基于服务能力的可用性模型

根据 4.2 节可知可重构网络系统 Γ 所构成的状态是一个具有平稳分布的不可分的遍历马尔科夫链，设 π_N、π_P 和 π_C 分别为各状态的唯一稳定分布，则根据平稳分布的定义可求得各状态的平均返回时间为其唯一稳定分布的倒数，即

$$\begin{aligned}\tau_N &= \frac{1}{\pi_N} = \left(1 + p_{PN} + p_{PC} + \frac{p_{NN}(1-P_{PP})}{p_{NP}} + \frac{p_{PC}(p_{CN}+p_{CC})}{1-p_{CC}}\right)\frac{p_{NP}}{1-p_{PP}} \\ \tau_P &= \frac{1}{\pi_P} = 1 + p_{PN} + p_{PC} + \frac{p_{NN}(1-p_{PP})}{p_{NP}} + \frac{p_{PC}(p_{CN}+p_{CC})}{1-p_{CC}} \\ \tau_C &= \frac{1}{\pi_C} = \left(1 + p_{PN} + p_{PC} + \frac{p_{NN}(1-p_{PP})}{p_{NP}} + \frac{p_{PC}(p_{CN}+p_{CC})}{1-p_{CC}}\right)\frac{1-p_{CC}}{p_{PC}}\end{aligned} \tag{19}$$

基于网络可用性的定义，在可重构网络系统 Γ 中，可用性即是系统处于可用状态的时间与总时间的比率，亦可表示为系统处于可用状态的概率。因此根据系统状态，可重构网络系统 Γ 的可用性 A 可表示为

$$A = \frac{\pi_N + \pi_P}{\pi_N + \pi_P + \pi_C} \tag{20}$$

即为

$$A = \frac{(1-p_{CC})(1-p_{PP}) + (1-p_{CC})p_{NP}}{(1-p_{CC})(1-p_{PP}) + (1-p_{CC})p_{NP} + p_{PC}p_{NP}} \tag{21}$$

根据式(18)和式(21)可知，网络系统 Γ 的可用性与网络节点数量 n、节点攻击成功的概率 ρ、阈值 k_{normal} 和 k_{fail} 以及节点重构成功率 γ 相关。

6　仿真分析

本节通过仿真实验对可重构网络系统的可用性模型进行模拟仿真，测试比较本文得到的理论模型与仿真实验结果的误差，分别模拟在不同参数条件下网络系统的可用性能。

6.1　模拟实验环境

实验环境为 Intel(R) Core(TM) i7 CPU 2.67 GHz, RAM 2 GB 的 PC 上，通过 C++编程模拟可重构网络的拓扑变化以及网络系统的重构。

1) 底层物理网络：拓扑结构有 GT-ITM 工具生成，物理网络包含 100 个节点，每个节点之间的链接概率为 10%，即网络系统初始拓扑中包含 500 条物理链路，可重构网络中的节点和链路资源取值在[50,100]内均匀分布。在进行仿真实验过程中，物理节点故障均发生在事先预定的时间点。

2) 服务承载网：仿真实验环境中，假设同时存在 20 个拥有随机拓扑结构的承载网运行在共享的底层网络上，每个承载网请求的节点个数在[2,8]内均匀分布，链路资源请求在[5,30]内均匀分布。基于上述实验环境，分别预设 10、20、30 次虚拟设备故障，这些故障会在每个固定的时间按顺序发生，发生故障的节点通过重构机制以先到先服务的方式进行顺序恢复。

6.2　数据分析

为了验证系统可用性与攻击成功率之间的关系并简化实验，假设实验中单节点的攻击成功率与网络规模无关，是一个固定的常数。

实验设置节点个数 m 和参数 k_{normal}（图中标示为 k_1）、k_{fail}（图中标示为 k_2）固定，分别在不同的单节点攻击成功率条件下对不同的重构成功率参数进行仿真，将上述可用性模型与仿真实验结果进行比较，其可用性 A 的变化曲线如图 3 所示。

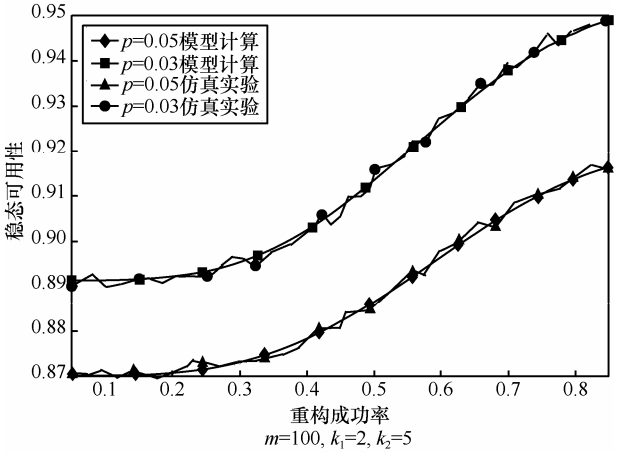

图 3　网络可用性与重构成功率的关系

实验验证可用性与网络规模的关系。随着网络规模的改变网络系统状态跳转的节点数量也不同，即参数 k_{normal} 和 k_{fail} 会随着网络规模变化，因此实验设置状态跳转的阈值比率不变，即分别从状态 N 到状态 P 及从状态 P 到状态 C 时，失效节点与总节点数的比值不变（图中标示为 p_1，p_2），同时设置

节点重构成功率 γ 不变，分别在不同的单节点攻击成功率条件下，对不同的网络规模进行仿真，将上述可用性模型与仿真实验结果进行比较，其可用性 A 的变化曲线如图 4 所示。

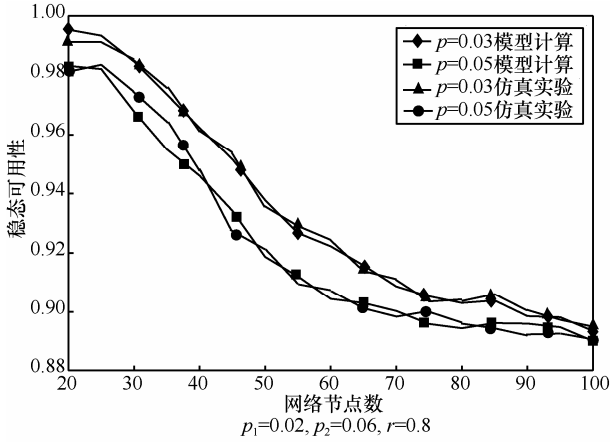

图 4 网络可用性与网络规模的关系

对可用性模型进行分析可知，对单个节点的攻击成功率越高，则系统可用性越低；另一方面，故障恢复能力越强，即节点重构成功率越高，则系统可用性越高。从直观上分析，也不难得到类似的结论，根据仿真实验（如图 3 和图 4 所示）亦可证明上述结论的正确性。

综上，根据仿真实验结果与模型计算结果的对比，分析得到如下结论。

1) 仿真实验得到的结果与模型计算结果具有很好的拟合性，即本文得到的系统可用性模型在预测特定条件下的可重构网络系统可用性方面具有较高的准确性，基于该模型的预测指标可以用于指导基于特定可用性需求的可重构网络构建。

2) 可重构网络的可用性能与重构成功率密切相关。由图 3 可知，重构成功率越高，则网络系统的可用性能越好。因此在网络规模一定、网络有效运行的判定条件不变的条件下，如果可以优化故障恢复算法，有效提高故障节点的重构成功率，则能够提高整个网络系统的可用性能。

3) 可重构网络的可用性能与节点攻击成功率密切相关。如图 3 和图 4 所示，节点攻击成功率越高，则网络系统的可用性能越差。因此，应该增强节点的防攻击性能，使尽量减小节点被成功攻击的概率，则可以提升整个网络系统的可用性能。

4) 可重构网络系统的规模对可用性能产生影响。如图 4 所示，在相同节点重构成功率条件下，随着网络规模的增大其可用性水平是逐渐降低的。如果将网络规模理解为网络系统的质量，则系统中的节点数量越大，即网络规模越大，则其质量也越大，其惯性也越大，如果一旦进入不可用状态，在相同的单个节点重构成功率前提下也越不容易恢复为正常状态。

7 结束语

本文研究了可重构网络系统的运行状态，通过对节点服务能力和网络服务能力的定量描述，构建了可重构网络系统中各状态的转移概率矩阵，从而给出网络系统的可用性模型。通过仿真实验对该可用性模型的有效性进行验证，仿真结果表明，理论模型计算结果与仿真结果拟合性较好，可用于描述特定可重构网络的可用性能。通过对该可用性模型的分析可知，为了提高可重构网络系统的可用性能，可以从多个方面进行改进，包括：1) 降低单个节点被成功攻击的概率；2) 提高节点失效情况下快速恢复的能力；3) 有效控制网络规模爆炸式增长。

参考文献：

[1] 程东年, 汪斌强, 王保进等. 网络结构自调整的柔性内涵初探[J]. 通信学报, 2012,8(33): 214-222.
CHENG D N, WANG B Q, WANG B J, *et al*. Preliminary study on the connotation of flexibility in dynamically reconfigurable networks[J]. Journal on Communications, 2012, 8(33):214-222.

[2] 兰巨龙, 邢池强, 胡宇翔等. 可重构技术与未来网络体系架构[J]. 电信科学, 2013, 29(8):16-23.
LAN J L, XING C Q, HU Y X, *et al*. Reconfiguration technology and future network architecture[J]. Telecommunications Science, 2013, 29(8):16-23.

[3] 兰巨龙, 程东年, 胡宇翔. 可重构信息通信基础网络体系研究[J]. 通信学报, 2014, 35(1):128-139.
LAN J L, CHENG D N, HU Y X. Research on reconfigurable information communication basal network architecture[J]. Journal on Communications, 2014, 35(1):128-139.

[4] 齐宁, 汪斌强, 郭佳. 逻辑承载网构建方法的研究[J]. 计算机学报, 2010, 33(9):1533-1540.
QI N, WANG B Q, GUO J. Research on construction methods of logical carrying network[J]. Chinese Journal of Computers, 2010, 33(9):1533-1540.

[5] 王志明等. 可重构服务承载网容错构建算法研究[J]. 电子与信息学报, 2012,34(2):54-56.
WANG Z M, *et al*. Research on reconfigurable service carrying net-

work resilient construction algorithms[J]. Journal of Electronics & Information Technology, 2012, 34(2):54-56.

[6] 林闯, 汪洋, 李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005, 28(12):1944-1956.
LIN C WANG Y, LIN Q L. Stochastic modeling and evaluation for network security[J]. Chinese Journal of Computers, 2005, 28(12): 1944-1956.

[7] NICOL D M, SANDERS W H, TRIVEDI K S. Model-based evaluation: From dependability to security[J]. IEEE Transactions on Dependability and Security, 2004, 1(1): 48-65.

[8] 原菊梅. 复杂系统可靠性 Petri 网建模及智能分析方法[M]. 北京: 国防工业出版社, 2011.
YUAN J M. Reliability Petri Net Modeling of Complex Systems and Intelligent Analysis[M]. Beijing: Defense Industry Press, 2011.

[9] 王健, 王慧强, 赵国生. 信息系统可生存性定量评估的指标体系[J]. 计算机工程，2009,35(3):54-56.
WANG J, WANG H Q, ZHAO G S. Index system of quantitative evaluation for information systems survivability[J]. Computer Engineering, 2009,35(3): 54-56.

[10] 陈秀真, 郑庆华等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4):885-897.
CHEN X Z, ZHENG Q H, *et al*. Quantitative hierarchical threat evaluation model for network security[J]. Jorunal of Software, 2006, 17(4): 885-897.

[11] 姜伟, 方滨兴等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4):817-827.
JIANG W, FANG B X, *et al*. Evaluating network security and optimal active defense based on attack2defense game model[J]. Chinese Journal of Computers, 2009，32(4):817-827.

[12] MCDERMOTT J. Attack-potential-based survivability modeling for high-consequence systems[A]. Proceedings of the 3rd IEEE International Workshop on Information Assurance(IWIA'05)[C]. Callege Park, Maryland, USA, 2005.119-130.

[13] 冯萍慧, 连一峰. 基于可靠性理论的分布式系统脆弱性模型[J]. 软件学报, 2006, 17(7):1633-1640.
FENG P H, LIAN Y F. A vulnerability model of distributed systems based on reliability theory[J]. Journal of Software, 2006,17(7): 1633-1640.

[14] GOSEVA.P K, WANG F, WANG R. Characterizing intrusion tolerant systems using a state transition model[A]. Proceedings of DARPA DISCEX II Conference[C]. 2001.211-221.

作者简介：

赵靓（1979-），女，山西盂县人，博士，国家数字交换系统工程技术研究中心工程师、讲师，主要研究方向为新一代信息网络关键技术与理论。

张校辉（1979-），男，河南洛阳人，博士，国家数字交换系统工程技术研究中心工程师、讲师，主要研究方向为面向三网融合的下一代信息网络关键技术、软件定义网络等。

王雨（1975-），男，河南郑州人，硕士，国家数字交换系统工程技术研究中心工程师、讲师，主要研究方向为新一代信息网络硬件平台关键技术。