第 38 卷 第 2 期
Vol.38 No.2

计 算 机 工 程
Computer Engineering

2012 年 1 月
January 2012

• 博士论文 •

文章编号：1000—3428(2012)02—0014—03 文献标识码：A 中图分类号：TP393

基于着色 Petri 网的系统可生存性仿真平台

李良斌[1,2]，王劲林[2]，陈 君[2]

(1. 中国科学院研究生院，北京 100049；2. 中国科学院声学研究所国家网络新媒体工程技术研究中心，北京 100190)

摘 要：对可生存系统组件在攻击、抵抗、恢复 3 种因素作用下的状态转换过程进行分析，设计基于着色 Petri 网的系统可生存性仿真平台，从攻击强度、攻击密度、恢复强度、攻击策略、恢复策略 5 个方面模拟可生存系统的行为特性。以一个 IPTV 网络服务系统为例，利用平台仿真其在遭受不同攻击时的服务提供能力。仿真结果表明，该平台能较好地实现系统可生存性分析。

关键词：可生存性；分布式服务系统；仿真平台；攻击；恢复；着色 Petri 网

Simulation Platform for System Survivability Based on Coloured Petri Net

LI Liang-bin[1,2], WANG Jin-lin[2], CHEN Jun[2]

(1. Graduate University of Chinese Academy of Sciences, Beijing 100049, China;
2. National Network New Media Engineering Research Center, Institute of Acoustics, Chinese Academy of Sciences, Beijing 100190, China)

【Abstract】By analyzing the state transition process of components of survivable system under action of attack, resistance and recovery, this paper designs the simulation platform for system survivability based on Coloured Petri Net(CPN), which simulates the behavior of survivable system from aspects of attack intensity, attack density, recovery intensity, attack strategy and recovery strategy. The structure and operating mechanism of the platform is illustrated in detail, and by using an IPTV network service system as an example, it simulates its service delivery capacity under different attacks with the platform. Simulation results show it can realize the survivability analysis well.

【Key words】survivability; distributed service system; simulation platform; attack; recovery; Coloured Petri Net(CPN)

DOI: 10.3969/j.issn.1000-3428.2012.02.005

1 概述

互联网的普及使网络服务系统日益呈现出大规模、分布化的趋势，一方面服务的提供必须依靠多个组件协同配合，另一方面传统安全保障技术的堡垒式防御模型已无法满足需求。可生存性理论[1]为解决分布式系统的安全保障问题提供了新的思路。与传统技术不同，可生存性理论承认组件的失效是不可避免的，因此，不再追求系统的绝对安全，而重点关注系统在任意组件失效情况下的服务提供能力。为了满足该需求，可生存系统通常采用冗余的方法为每种组件维持多个实例。组件实例必须具有对攻击的抵抗能力，同时系统还应具备恢复功能对失效的组件实例进行恢复。因此，可生存系统的运作过程可以看作攻击、抵抗、恢复 3 种因素并行作用的过程。

为了分析及增强系统的可生存性，有必要通过仿真手段对系统的行为特性进行模拟。文献[2]基于 PRISM 语言构建了系统行为的概率模型，进而采用概率模型检验技术研究系统的可生存性，但该方法对系统在多种因素并行作用下的时序特征描述能力不足；文献[3]提出了基于着色 Petri 网(Coloured Petri Net, CPN)的可生存系统建模方法，但该方法仅从组件的失效率及恢复率 2 个方面模拟系统行为，无法精确表达攻击的到达特性及单次攻击的强度对系统的影响。本文通过对可生存系统的组件在攻击、抵抗、恢复 3 种因素作用下的状态转换过程进行分析，设计了基于着色 Petri 网的系统可生存性仿真平台，该平台从攻击强度、攻击密度、恢复强度、攻击策略、恢复策略 5 个方面模拟可生存系统的行为特性。

2 组件状态的转换过程

在对组件的状态转换过程进行阐述之前，参照文献[3-4]做出以下合理假设：(1)攻击的到达可以采用泊松过程进行建模；(2)攻击直接作用于组件实例，任意组件实例都无法做到绝对安全，即在持续攻击的作用下最终都将失效，从攻击到达到组件失效的时间服从负指数分布；(3)对于失效的组件实例，系统采用恢复功能对其进行恢复，从开始恢复到恢复成功的时间同样服从负指数分布。

观察攻击的到达时刻，系统遭受的攻击可以看作时间轴上的冲击函数序列。设相邻 2 个冲击到达的时间间隔为 θ，则当攻击按照泊松过程到达时，θ 为符合负指数分布的随机变量，设其均值为 θ_0，θ_0 反映了系统遭受攻击的密度。同时本文采用攻击强度 η 对单次攻击进行表达，攻击强度体现了攻击者的能力，进而表达其对系统的破坏效果，设 η 满足正态分布，其均值与方差分别为 η_0 和 σ_0。因此，系统遭受的攻击可以采用三元组 $(\theta_0,\eta_0,\sigma_0)$ 唯一确定，在本文的实验部分，通常取 $\sigma_0=\eta_0\times0.15$。

抵抗力是可生存系统的重要特性，反映了系统对攻击的

基金项目：国家“863”计划基金资助项目“新一代业务运行管控协同支撑环境的开发”(2008AA01A317)

作者简介：李良斌(1985－)，男，博士研究生，主研方向：网络安全；王劲林，研究员、博士生导师；陈 君，副研究员

收稿日期：2011-06-16 **E-mail：**lilb@dsp.ac.cn

防御效果。定义从攻击到达到组件实例失效的时间为攻击失效时间，用 t 表示，则 t 为满足负指数分布的随机变量，其均值取决于攻击与抵抗能力的对比。定义组件实例的防御参量 λ，当攻击强度为 η 的攻击作用于该组件时，t 应该与 λ 呈正比且与 η 呈反比，则 t 的均值可以用 $\alpha\lambda/\eta$ 表达，α 为调整因子，本文取 $\alpha=1$，t 的概率密度函数可以表示为：

$$f(t)=\frac{\eta}{\alpha\lambda}\mathrm{e}^{-\eta t/\alpha\lambda},\ t>0 \tag{1}$$

当组件实例失效时，系统采用恢复功能对其进行恢复。定义从开始恢复到恢复成功的时间为失效恢复时间，用 τ 表示，τ 同样为满足负指数分布的随机变量，其均值取决于组件本身的特性及系统的恢复能力。定义系统的恢复强度 μ，则 τ 应该与 μ 呈反比。此外 τ 应正比于组件实例的抵抗参量 λ，这是由于该结论的依据为，抵抗参量的提升往往依赖于复杂组件结构，因此会带来更大的恢复难度。综上，τ 的均值可以采用 $\beta\lambda/\mu$ 表达，β 为调整因子，本文取 $\beta=1$，则 τ 的概率密度函数可以表示为：

$$f(\tau)=\frac{\mu}{\beta\lambda}\mathrm{e}^{-\mu\tau/\beta\lambda},\ \tau>0 \tag{2}$$

3　仿真平台设计

可生存系统的运作受到攻击、抵抗、恢复 3 个因素同时作用，仿真平台必须对系统在并行因素作用下的时序特性进行有效的模拟。着色 Petri 网[5]是一种图形化的建模工具，基于其对并行及随机性问题的强大描述能力，着色 Petri 网在系统仿真领域得到了广泛应用。因此，本文采用着色 Petri 网对可生存系统的运作过程进行建模，并基于 CPN Tools[6]设计了仿真环境。

首先必须对组件实例进行表示，参考文献[3]，采用标记(token)表示组件实例，标记的颜色代表其类型及抵抗参量。为了区分组件实例的状态，设置 2 个库所(place)N-Comps 和 F-Comps 分别用于存储状态正常及失效的组件实例。则攻击与恢复过程可以理解为将代表组件实例的标记分别按照相反的方向在上述 2 个库所之间移动，采用替代变迁 Attack 和 Recover 分别表示攻击和恢复过程。为了对攻击及恢复策略进行模拟，将库所 N-Comps 及 F-Comps 的颜色集 COMPS 定义为组件实例的 list 类型，且分别采用双向弧将其与替代变迁 Attack 及 Recover 相连接，当替代变迁 Attack 或 Recover 激发时，可以获得相应组件实例的全集，进而按照攻击或恢复策略选中某一组件实例，并将剩余的组件实例重新输出至相应库所。为了模拟攻击按照泊松过程到达的特性，采用一个单独的替代变迁 Attack Arrival 控制 Attack 的激发(fire)。同时为了反映系统的当前状态，设置库所 Comp Status 用于存储各个组件类型对应的正常的组件实例的数量，其颜色集 STATUS 被定义为 record 类型。图 1 展示了 CPN Tools 风格的仿真平台总体结构，其中，变迁 Sample 及库所 Sample Controller 与系统的行为逻辑无关，其作用是控制监控器(monitor)以对系统状态进行均匀采样。

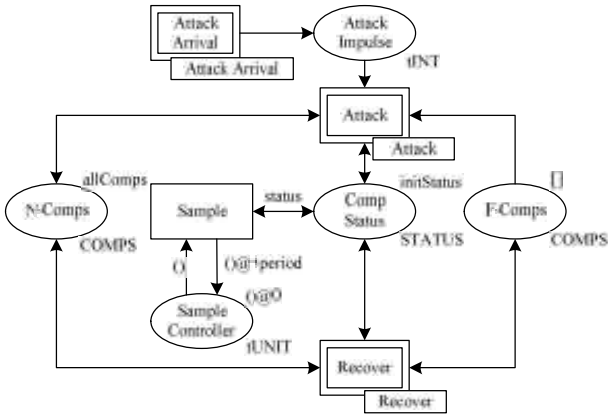


图 1　仿真平台总体结构

如上所述，替代变迁 Attack Arrival 用于控制攻击按照泊松过程到达，即相邻 2 次攻击的间隔服从负指数分布。如图 2 所示，本文采用库所 Next Arrival、Attack Impulse 和变迁 Arrive 实现该目的。在变迁 Arrive 激发时，向库所 Attack Impulse 输出标记代表本次攻击到达，同时通过指向库所 Next Arrival 的弧对输出标记的时间戳增加一个负指数分布的随机时延，从而模拟下一次攻击的到达时刻。为了模拟攻击强度的正态分布特性，图 2 中库所 Next Arrival 及 Attack Impulse 的颜色集表示攻击强度，并采用函数 normEta 随机产生符合正态分布的攻击强度值。

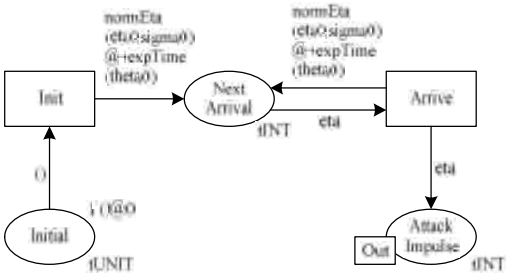


图 2　替代变迁 Attack Arrival

如图 3 所示，替代变迁 Attack 表示攻击过程。首先攻击必须受到替代变迁 Attack Arrival 的控制，其次还应体现攻击的组件实例选取策略。采用变迁 Prepare Attack 模拟这一特性，该变迁的激发受到库所 Attack Impulse 的控制。

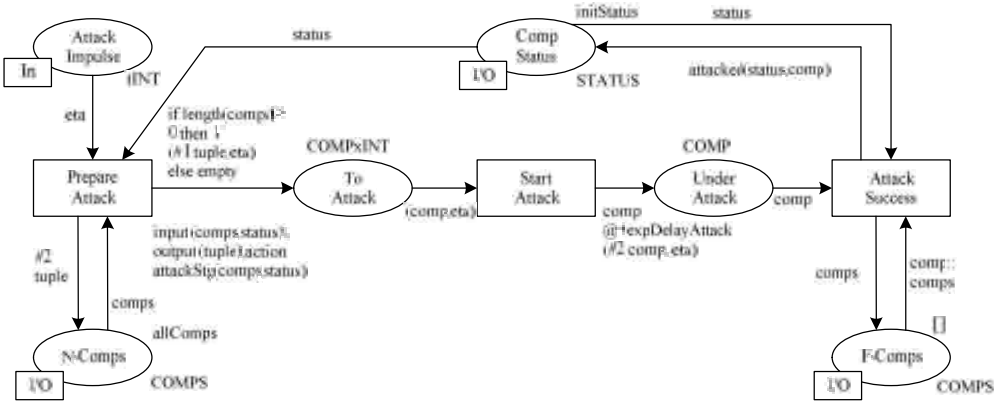


图 3　替代变迁 Attack

此外该变迁通过在代码段注释(code segment inscription)中调用函数 attackStg 模拟按照攻击策略从组件实例列表中选取攻击目标，图中 attackStg 的返回值 tuple 的颜色集被定义为组件及组件列表的乘积，前一个元素代表选中的组件实例，后一个元素代表其余的组件实例列表。选中的组件实例被输出至库所 To Attack，接着采用变迁 Start Attack、库所 Under Attack 及变迁 Attack Success 分别表示攻击开始、组件正在被攻击以及攻击成功，为表示攻击失效时间，图中变迁 Start Attack 至库所 Under Attack 的弧按照式(1)产生一个负指数分布的随机时延。攻击成功后需要对系统组件的状态进行相应的修改，因此，变迁 Attack Success 的激发在将代表组件实例的标记输出至库所 F-Comps 的同时，通过连接至库所 Comps Status 的弧实现组件状态的修改。

替代变迁 Recover 表示恢复过程，该替代变迁与 Attack 有类似的结构。如图 4 所示，为表示恢复策略，变迁 Prepare Recover 通过在代码段注释中调用函数 recoveryStg 模拟按照恢复策略从组件实例列表中选取攻击目标。与攻击按照泊松过程到达不同，当存在失效的组件实例时，即应当启动恢复过程，但恢复必须串行进行，为此采用反馈控制库所 Recover Controller 模拟这一特性。失效恢复时间的模拟同样通过在图中变迁 Start Recover 至库所 Under Recover 的弧上按式(2)产生一个负指数分布的随机时延来表示。

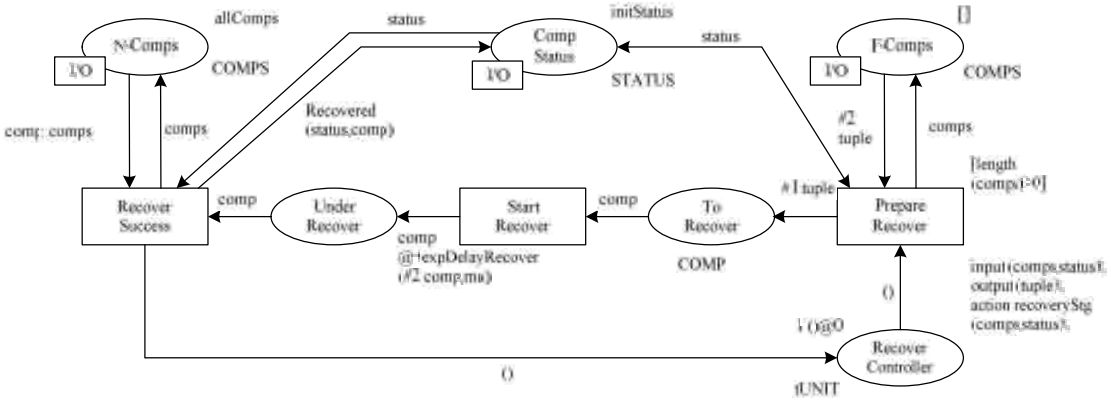


图 4 替代变迁 Recover

4 实验及分析

4.1 实例系统

为了进一步阐述本仿真平台的使用方法，本节以一个 IPTV 网络服务系统为例，对其在遭受不同攻击时的服务提供能力进行仿真。如图 5 所示，该系统包括 7 种组件，各种组件按照一定的结构进行连接，并通过它们的交互为用户提供服务。为了对问题进行简化，假设同一类型的组件实例具有相同的抵抗参量，图中括号内的信息分别表示组件的简称、抵抗参量以及初始状态下组件实例的个数。

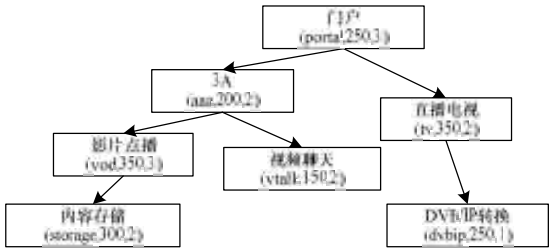


图 5 IPTV 网络服务系统组件架构

按照用户对系统功能的感知以及系统的应用逻辑，该系统可以提供 3 项用户可以感知的服务，表 1 列出了服务名称及其所依赖的组件。

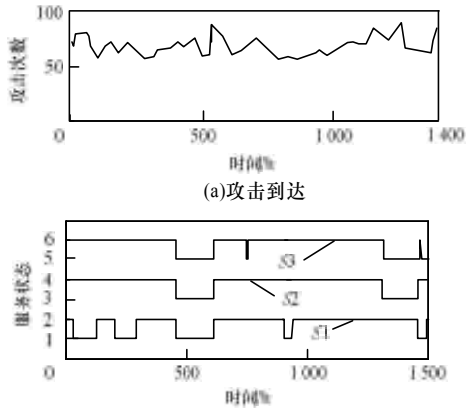
表 1 IPTV 网络服务系统提供的服务及其依赖的组件

服务	依赖组件
S1 直播电视	portal, tv, dvbip
S2 视频聊天	portal, aaa, vtalk
S3 影片点播	portal, aaa, vod, storage

可生存性重点关注系统遭受攻击时服务的提供能力，为此为每个服务设置对应的监控器。监控器与库所 Comp Status 及变迁 Sample 相关联，通过分析组件的状态对服务是否可用进行判定，当服务依赖的所有组件都存在至少一个功能正常的组件实例时，则判定该服务可用。

4.2 仿真结果

考虑攻击者采用随机攻击策略且系统采用随机恢复策略，图 6 展示了 $\theta_0=30$、$\eta_0=55$、$\mu=12$ 时攻击到达情况及其对应的服务可用情况。图 6(b)中服务状态取偶数表示服务可用，取奇数表示服务不可用。从图中可以看出，当攻击作用于系统时，部分服务的状态变为不可用，之后通过恢复功能可以恢复至攻击前的水平，服务的可用情况随时间呈现出随机波动的特性，这符合实际网络环境中系统服务提供能力的变化。



(a)攻击到达

(b)服务状态

图 6 攻击到达与服务状态对照

为了反映系统的总体运行情况，接下来的实验重点考察服务状态为可用的概率，为此分别采用 1 和 0 表示服务状态为可用和不可用，并对观察到的服务状态值在时间上取平均。在取平均值之前，令着色 Petri 网执行 50 步。表 2 展示了恢复强度 $\mu=12$ 时，系统在不同参数攻击的作用下各项服务状

(下转第 20 页)